Cisco Security Appliance コマンド リファレンス

Cisco ASA 5500 シリーズ /Cisco PIX 500 シリーズ用

ソフトウェア バージョン 8.0(5)

Text Part Number: OL-12173-02-J

このマニュアルについて

ここでは、『*Cisco Security Appliance コマンド リファレンス*』について紹介します。

この前書きは、次の項で構成されています。

マニュアルの目的

このマニュアルでは、ネットワークの不正利用を防いだり、リモート サイトとユーザをネットワークに接続するバーチャル プライベート ネットワークを設定したりするための、セキュリティ アプライアンスで使用できるコマンドについて説明します。

セキュリティ アプライアンスの設定とモニタは、ASDM（Web ベースの GUI アプリケーション）を使用して行うこともできます。ASDM には、一般的なコンフィギュレーション シナリオに基づいて誘導するコンフィギュレーション ウィザードと、あまり一般的でないシナリオ向けのオンライン ヘルプがあります。詳細については、http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm を参照してください。

このマニュアルは、Cisco PIX 500 シリーズのセキュリティ アプライアンス（PIX 515/515E、PIX 525、および PIX 535）および Cisco ASA 5500 シリーズのセキュリティ アプライアンス（ASA 5505、ASA 5510、ASA 5520、ASA 5540、および ASA 5550）に適用されます。このマニュアルを通じて、「セキュリティ アプライアンス」という語は、特に指定がなければ、一般的にサポートされているすべてのモデルに適用されます。PIX 501、PIX 506E、および PIX 520 セキュリティ アプライアンスは、ソフトウェア バージョン 8.0 でサポートされていません。

対象読者

このマニュアルは、次の作業を担当するネットワーク管理者を対象としています。

- ネットワーク セキュリティの管理
- ファイアウォールおよびセキュリティ アプライアンスのインストールと設定
- VPN の設定
- 侵入検知ソフトウェアの設定

このマニュアルと『*Cisco Security Appliance Command Line Configuration Guide*』を併せて使用してください。

マニュアルの構成

- 「コマンドライン インターフェイスの使用」では、セキュリティ アプライアンス コマンドとアクセス コマンドを紹介します。
- 第 1 章から第 32 章では、すべてのコマンドをアルファベット順に説明します。

表記法

セキュリティ アプライアンスのコマンド構文の説明には、次の表記法を使用しています。

コマンドの説明では、次の表記法を使用しています。

- 波カッコ（{ }）は、選択すべき必須の要素を示します。
- 角カッコ（[ ]）は、省略可能な要素を示します。
- 縦線（|）は、二者択一、つまりどちらか一方を選択する要素を区切ります。
- 記載されているとおりに入力するコマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。

例を挙げて説明する場合は、次の表記法を使用しています。

- 画面に表示される情報は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の** `screen` フォントで示しています。
- ユーザが値を指定する変数は、*イタリック体の* `screen` フォントで示しています。
- 例には、異なるプラットフォームでの出力結果が含まれることがあります。たとえば、ご使用のプラットフォームでは使用できないために、例に表示されるインターフェイス タイプを認識できない場合があります。相違点は軽微なものになっています。

（注） 「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

モード、プロンプト、および構文の詳細については、第　章「コマンドライン インターフェイスの使用」を参照してください。

関連資料

詳細については、次のマニュアルを参照してください。

- 『*Cisco Security Appliance Command Line Configuration Guide*』
- 『*Cisco ASA 5500 Series Release Notes*』
- 『*Release Notes for Cisco ASDM*』
- 『*Cisco ASA 5580 Adaptive Security Appliance Getting Started Guide*』
- 『*Cisco ASA 5500 Series Hardware Maintenance Guide*』
- 『*Cisco ASA 5500 Getting Started Guide*』
- 『*Cisco ASA 5505 Getting Started Guide*』
- 『*Cisco PIX Security Appliance Release Notes*』
- 『*Cisco PIX 515E Quick Start Guide*』
- 『*Cisco Security Appliance System Log Messages*』
- 『*Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*』
- 『*Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*』
- 『*Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*』
- 『*Release Notes for Cisco Secure Desktop*』
- 『*Migration Guide for Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations*』
- 『*Migrating to ASA for VPN 3000 Concentrator Series Administrators*』
- 『*Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

コマンドライン インターフェイスの使用

この章では、セキュリティ アプライアンスでの CLI の使用方法について説明します。この章は次の内容で構成されています。

（注） この CLI では構文など、Cisco IOS CLI と類似した表記法を使用しますが、セキュリティ アプライアンスのオペレーティング システムが Cisco IOS ソフトウェアのいずれかのバージョンに該当するわけではありません。Cisco IOS CLI コマンドがセキュリティ アプライアンスで動作するわけでも、同じ機能を使用できるわけでもありませんので注意してください。

ファイアウォール モードとセキュリティ コンテキスト モード

セキュリティ アプライアンスは、次のモードの組み合わせで動作します。

- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード

  ファイアウォール モードは、セキュリティ アプライアンスがレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールのいずれとして動作するかを決定します。
- マルチ コンテキスト モードまたはシングル コンテキスト モード

セキュリティ コンテキスト モードは、セキュリティ アプライアンスが単一のデバイスとして動作するか、またはマルチセキュリティ コンテキストとして動作する（仮想デバイスのように動作する）かを決定します。

特定のモードでしか使用できないコマンドもあります。

コマンドのモードとプロンプト

セキュリティ アプライアンスの CLI にはコマンド モードが含まれています。特定のモードでしか入力できないコマンドもあります。たとえば、機密情報を表示するコマンドを入力するには、パスワードを入力して特権モードに入る必要があります。次に、コンフィギュレーション変更が誤って入力されないようにするために、コンフィギュレーション モードに入る必要があります。下位のコマンドはすべて、高位のモードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力することができます。

システム コンフィギュレーション モードまたはシングル コンテキスト モードに入っている場合、プロンプトはホスト名で始まります。

```
hostname
```

コンテキスト内に入っている場合、プロンプトはホスト名で始まり、その後にコンテキスト名が続きます。

```
hostname/context
```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

  ユーザ EXEC モードでは、最小限の セキュリティ アプライアンス 設定が表示されます。ユーザ EXEC モードのプロンプトは、初めて セキュリティ アプライアンス にアクセスしたときに次のように表示されます。

  ```
  hostname>

  hostname/context>
  ```

- 特権 EXEC モード

  特権 EXEC モードでは、ユーザの特権レベルまでの現在の設定がすべて表示されます。すべてのユーザ EXEC モード コマンドは、特権 EXEC モードで動作します。特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを入力します。これにはパスワードが必要です。プロンプトにはシャープ記号（#）が含まれています。

  ```
  hostname#

  hostname/context#
  ```

- グローバル コンフィギュレーション モード

  グローバル コンフィギュレーション モードでは、セキュリティ アプライアンス コンフィギュレーションを変更できます。このモードでは、ユーザ EXEC、特権 EXEC、およびグローバルの各コンフィギュレーション コマンドをすべて使用できます。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードで **configure terminal** コマンドを入力します。プロンプトが次のように変化します。

  ```
  hostname(config)#

  hostname/context(config)#
  ```

- コマンド固有のコンフィギュレーション モード

  いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバルの各コンフィギュレーション コマンド、およびコマンド固有のコンフィギュレーション コマンドをすべて使用できます。たとえば、**interface** コマンドを使用すると、インターフェイス コンフィギュレーション モードに入ります。プロンプトが次のように変化します。

  ```
  hostname(config-if)#

  hostname/context(config-if)#
  ```

構文の書式

コマンド構文の説明には、次の表記法を使用しています。

表 1　　構文の表記法

表記法	説明
太字	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの短縮形

ほとんどのコマンドは、コマンドに固有の最小文字数まで短縮できます。たとえば、コンフィギュレーションを表示するには、完全なコマンド **write terminal** を入力する代わりに、**wr t** と入力できます。または、特権モードを開始するには **en**、コンフィギュレーション モードを開始するには **conf t** と入力できます。さらに、**0** を入力して、**0.0.0.0** を表すことができます。

コマンドラインの編集

セキュリティ アプライアンスでは、Cisco IOS ソフトウェアと同じコマンドライン編集ルールが使用されます。**show history** コマンドを使用して以前入力した全コマンドを表示することも、↑ キーまたは **^p** コマンドで 1 つずつ前のコマンドを表示することもできます。前に入力したコマンドを確認したら、

↓キーまたは **^n** コマンドでリスト内で前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、**Enter** キーを押して実行することもできます。**^w** でカーソルの左側にある単語を削除することも、**^u** でカーソルのある行を消去することもできます。

セキュリティ アプライアンスでは、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

コマンドの補完

部分的な文字列を入力してからコマンドまたはキーワードを完成させるには、**Tab** キーを押します。セキュリティ アプライアンスは、部分的な文字列がコマンドまたはキーワード 1 つだけと一致する場合に限り、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して **Tab** キーを押した場合は、一致するコマンドが複数あるため、セキュリティ アプライアンスはコマンドを完成させません。ただし、**dis** を入力して Tab キーを押すと、コマンド **disable** が補完されます。

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*

  特定のコマンドのヘルプを表示します。

- **help ?**

  ヘルプがあるコマンドを表示します。

- *command_name* **?**

  使用可能な引数のリストを表示します。

- *string***?**（スペースなし）

  その文字列で始まるコマンドをリストします。

- **?** および **+?**

  使用できるすべてのコマンドをリストします。**?** と入力すると、セキュリティ アプライアンスは現在のモードで使用できるコマンドだけを表示します。下位モードのコマンドも含め、使用できるすべてのコマンドを表示するには、**+?** と入力します。

（注） コマンド ストリングに疑問符（?）を含める場合は、不用意に CLI ヘルプが起動しないよう、疑問符を入力する前に Ctrl+V を押す必要があります。

show コマンド出力のフィルタリング

縦棒（|）はどの **show** コマンドでも使用できます。これには、フィルタ オプションとフィルタリング式を組み込むことができます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現と照合することによって行われます。選択するフィルタ オプションによって、正規表現に一致するすべての出力を含めたり除外したりできます。また、正規表現に一致する行で始まるすべての出力を表示することもできます。

show コマンドでフィルタリング オプションを使用する場合の構文は、次のとおりです。

```
hostname# show command | {include | exclude | begin | grep [-v]} regexp
```

このコマンド文字列の最初の縦棒（|）は演算子であり、コマンド内に含める必要があります。この演算子は、**show** コマンドの出力をフィルタに誘導します。構文内に含まれるその他の縦棒（|）は代替オプションを示すものであり、コマンドの一部ではありません。

include オプションを指定すると、正規表現に一致するすべての出力行が表示されます。**-v** を付けずに **grep** オプションを使用する場合も、同じ結果となります。**exclude** オプションを指定すると、正規表現に一致するすべての出力行が除外されます。**-v** を付けて **grep** オプションを使用する場合も、同じ結果となります。**begin** オプションを指定すると、正規表現に一致する行で始まるすべての出力行が表示されます。

regexp には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、*メタ文字*と呼ばれるキーボード文字は、正規表現で使用されると特別な意味を持ちます。

Ctrl キーを押した状態で **V** キーを押すと、CLI において、疑問符（?）やタブなどの特殊文字をすべてエスケープできます。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

表 2 は、特殊な意味を持つメタ文字のリストです。

表 2　　regex メタ文字

文字	説明	注意事項
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp*)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）** Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。

表 2　　regex メタ文字 （続き）

文字	説明	注意事項
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc***]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。
[*a-c***]**	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

コマンド出力のページング

help、**?**、**show**、**show xlate** や、リストが長いその他のコマンドなどでは、画面に情報を表示して停止するか、完了するまでコマンドを実行させるかを指定できます。**pager** コマンドを使用すると、画面上に表示する行数を選択して、その行数を表示した後に More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトの構文は、UNIX の **more** コマンドと似ています。

- 次の 1 画面分の情報を表示するには、スペース バーを押します。

- 次の行を表示するには、Enter キーを押します。
- コマンドラインに戻るには、q キーを押します。

コメントの追加

行の先頭にコロン（:）を置いて、コメントを作成できます。しかし、コメントが表示されるのはコマンド ヒストリ バッファだけで、コンフィギュレーションには表示されません。したがって、コメントは、**show history** コマンドを使用するか、矢印キーを押して前のコマンドを取得することによって表示できますが、コンフィギュレーションには含まれないので、**write terminal** コマンドでは表示できません。

テキスト コンフィギュレーション ファイル

この項では、セキュリティ アプライアンスにダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。次の項目を取り上げます。

テキスト ファイルでコマンドと行が対応する仕組み

テキスト コンフィギュレーション ファイルには、このガイドで説明するコマンドに対応する行が含まれています。

例では、コマンドの前に CLI プロンプトがあります。次の例では、CLI プロンプトは「hostname(config)#」です。

```
hostname(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンドの入力を求めるプロンプトが表示されないので、プロンプトは省略されています。

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

コマンド固有のコンフィギュレーション モード コマンドは、コマンドラインで入力されたときに、メイン コマンドの下に字下げして表示されます。テキスト ファイルの行は、コマンドがメイン コマンドのすぐ後に表示される限り、字下げする必要はありません。たとえば、次のテキストは字下げされていませんが、字下げしたテキストと同じように読み取られます。

```
interface gigabitethernet0/0
```

```
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト入力

コンフィギュレーションをセキュリティ アプライアンスにダウンロードすると、セキュリティ アプライアンスにより一部の行が自動的に挿入されます。たとえば、セキュリティ アプライアンスは、デフォルト設定のため、またはコンフィギュレーションが変更されたときのための行を挿入します。テキスト ファイルを作成するときは、これらの自動入力を行う必要はありません。

行の順序

ほとんどの場合、コマンドはファイル内で任意の順序に置くことができます。ただし、ACE などいくつかの行は表示された順に処理されるので、順序がアクセス リストの機能に影響する場合があります。その他のコマンドでも、順序の要件がある場合があります。たとえば、あるインターフェイスの名前を多数の後続コマンドが使用する場合は、そのインターフェイスの **nameif** コマンドをまず入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドは、メイン コマンドの直後に置く必要があります。

テキスト コンフィギュレーションに含まれないコマンド

いくつかのコマンドは、コンフィギュレーションに行を挿入しません。たとえば、**show running-config** などのランタイム コマンドは、テキスト ファイル内に対応する行があります。

パスワード

ログイン パスワード、イネーブル パスワード、およびユーザ パスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化された形式は jMorNbK0514fadBh のようになります。コンフィギュレーション パスワードは暗号化された形式で別のセキュリティ アプライアンスにコピーできますが、そのパスワードの暗号を解読することはできません。

暗号化されていないパスワードをテキスト ファイルに入力した場合、コンフィギュレーションをセキュリティ アプライアンスにコピーしても、セキュリティ アプライアンスは自動的にパスワードを暗号化しません。セキュリティ アプライアンスがパスワードを暗号化するのは、**copy running-config startup-config** コマンドまたは **write memory** コマンドを使用して、コマンドラインから実行コンフィギュレーションを保存した場合のみです。

マルチセキュリティ コンテキスト ファイル

マルチ セキュリティ コンテキストの場合、コンフィギュレーション全体は次に示す複数の部分で構成されます。

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、セキュリティ アプライアンスの基本設定を示すシステム コンフィギュレーション

- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

  システム コンフィギュレーションには、それ自体のインターフェイスまたはネットワーク設定は含まれていません。代わりに、システムは、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするときなど）、管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングル コンテキスト モード コンフィギュレーションに似ています。システム コンフィギュレーションにはシステム限定のコマンド（全コンテキストのリストなど）が含まれており、その他の一般的なコマンド（多数のインターフェイス パラメータなど）は存在しない点で、システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なっています。

CHAPTER 2

aaa accounting コマンド～ accounting-server-group コマンド

aaa accounting command

CLI で **show** コマンド以外のコマンドを入力したときに TACACS+ アカウンティング サーバにアカウンティング メッセージを送信するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを入力します。コマンド アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

構文の説明

tacacs+-server-tag	**aaa-server protocol** コマンドで指定するように、アカウンティング レコードの送信先の TACACS+ サーバまたはサーバのグループを指定します。
privilege *level*	**privilege** コマンドを使用してコマンドの特権レベルをカスタマイズする場合、最小特権レベルを指定することによって、セキュリティ アプライアンスで処理の対象とするコマンドを制限できます。最小特権レベルよりも下のコマンドは、セキュリティ アプライアンスで処理の対象となりません。 **（注）** 廃止されたコマンドを入力して **privilege** キーワードをイネーブルにした場合、廃止されたコマンドのアカウンティング情報はセキュリティ アプライアンスによって送信されません。廃止されたコマンドを処理の対象とするには、**privilege** キーワードをディセーブルにします。CLI では数多くの廃止されたコマンドがまだ受け入れられています。これらのコマンドは、現在受け入れられるコマンドに CLI で変換される場合もあります。廃止されたコマンドは、CLI のヘルプまたはこのマニュアルには記載されていません。

デフォルト

デフォルトの特権レベルは 0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

aaa accounting command コマンドを設定すると、管理者が入力する **show** コマンド以外の各コマンドが記録され、アカウンティング サーバに送信されます。

例

次に、サポート対象のコマンドについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のグループからサーバに送信されることを指定する例を示します。

```
hostname(config)# aaa accounting command adminserver
```

関連コマンド

コマンド	説明
aaa accounting	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting console

管理者アクセスの AAA アカウンティングのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting console** コマンドを使用します。管理者アクセスの AAA アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

no aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

構文の説明

enable	特権 EXEC モードの開始と終了を示すアカウンティング レコードの生成をイネーブルにします。
serial	シリアル コンソール インターフェイスを介して確立される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
server-tag	**aaa-server protocol** コマンドで定義された、アカウンティング レコードの送信先のサーバ グループを指定します。有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。
ssh	SSH で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
telnet	Telnet で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

aaa-server コマンドで指定済みのサーバ グループの名前を指定する必要があります。

例

次に、イネーブル アクセスについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のサーバに送信されることを指定する例を示します。

```
hostname(config)# aaa accounting enable console adminserver
```

関連コマンド

コマンド	説明
aaa accounting match	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
aaa accounting command	管理者/ユーザが入力する各コマンド（または、指定した特権レベル以上のコマンド）が記録され、アカウンティング サーバに送信されることを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting include, exclude

セキュリティ アプライアンスを介した TCP または UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting include** コマンドを使用します。アカウンティングからアドレスを除外するには、**aaa accounting exclude** コマンドを使用します。アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスをアカウンティングから除外します。
include	アカウンティングが必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server host** コマンドで定義した AAA サーバ グループを指定します。
service	アカウンティングが必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port* • **udp**/*port*

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

アクセス リストで指定されているトラフィックのアカウンティングをイネーブルにするには、**aaa accounting match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa accounting include** および **exclude** コマンドを使用することはできません。その場合は、**aaa accounting match** コマンドを使用する必要があります。

例

次に、すべての TCP 接続でアカウンティングをイネーブルにする例を示します。

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

関連コマンド

コマンド	説明
aaa accounting match	アクセス リストで指定されているトラフィックのアカウンティングをイネーブルにします。
aaa accounting command	管理者アクセスのアカウンティングをイネーブルにします。
aaa-server host	AAA サーバを設定します。
clear configure aaa	AAA コンフィギュレーションをクリアします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting match

セキュリティ アプライアンス を介した TCP および UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting match** コマンドを使用します。トラフィックのアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

構文の説明

acl_name	**access-list** 名との照合によるアカウンティングが必要なトラフィックを指定します。アクセス リスト内の permit エントリはアカウンティングの対象となり、deny エントリはアカウンティングから免除されます。このコマンドは、TCP トラフィックおよび UDP トラフィックについてのみサポートされます。このコマンドを入力し、他のプロトコルを許可するアクセス リストをこのコマンドが参照している場合、警告メッセージが表示されます。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

AAA サーバ プロトコル コンフィギュレーション モードで **accounting-mode** コマンドを使用して同時アカウンティングをイネーブルにしない限り、アカウンティング情報はサーバ グループ内のアクティブなサーバにのみ送信されます。

aaa accounting match コマンドは、**aaa accounting include** および **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

例

次に、特定のアクセス リスト acl2 と一致するトラフィックのアカウンティングをイネーブルにする例を示します。

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

関連コマンド

コマンド	説明
aaa accounting include、exclude	コマンドで IP アドレスを直接指定することによって、アカウンティングをイネーブルにします。
access-list extended	アクセス リストを作成します。
clear configure aaa	AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication console

シリアル、SSH、HTTPS（ASDM）、または Telnet 接続でセキュリティ アプライアンス CLI にアクセスするユーザを認証するか、**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証するには、グローバル コンフィギュレーション モードで **aaa authentication console** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

構文の説明

enable	**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証します。
http	HTTPS でセキュリティ アプライアンスにアクセスする ASDM ユーザを認証します。RADIUS サーバまたは TACACS+ サーバを使用する場合、設定する必要があるのは HTTPS 認証のみです。デフォルトでは、このコマンドを設定しなくても、ASDM によってローカル データベースが認証に使用されます。

LOCAL	認証にローカル データベースを使用します。**LOCAL** の文字は大文字と小文字が区別されます。ローカル データベースが空の場合、次の警告メッセージが表示されます。
	`Warning:local database is empty! Use 'username' command to define local users.`
	コンフィギュレーション内にまだ **LOCAL** があるときにローカル データベースが空になった場合、次の警告メッセージが表示されます。
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。HTTPS 管理認証では AAA サーバ グループ用に SDI プロトコルがサポートされません。 *server-tag* に加えて **LOCAL** キーワードを使用すると、AAA サーバを使用できない場合にフォールバック方式としてローカル データベースを使用するようにセキュリティ アプライアンスを設定できます。**LOCAL** の文字は大文字と小文字が区別されます。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。
serial	シリアル コンソール ポートを使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
ssh	SSH を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
telnet	Telnet を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。

デフォルト

デフォルトでは、ローカル データベースへのフォールバックはディセーブルになっています。

aaa authentication telnet console コマンドが定義されていない場合は、セキュリティ アプライアンスのログイン パスワード（**password** コマンドで設定）で、セキュリティ アプライアンス CLI にアクセスできます。

aaa authentication http console コマンドが定義されていない場合は、ユーザ名およびセキュリティ アプライアンスのイネーブル パスワード（**enable password** コマンドで設定）なしで、セキュリティ アプライアンスに（ASDM 経由で）アクセスできます。**aaa** コマンドが定義されているが、HTTPS 認証によってタイムアウトが要求される場合（AAA サーバがダウンしているか使用できないことを意味する）は、デフォルトの管理者ユーザ名とイネーブル パスワードを使用してセキュリティ アプライアンスにアクセスできます。デフォルトでは、イネーブル パスワードは設定されていません。

aaa authentication ssh console コマンドが定義されていない場合、ユーザ名 **pix** とセキュリティ アプライアンスのイネーブル パスワード（**enable password** コマンドで設定）を使用してセキュリティ アプライアンス CLI にアクセスできます。デフォルトでは、イネーブル パスワードは空白です。この動作は、AAA を設定しないでセキュリティ アプライアンスにログインする場合とは異なります。その場合は、ログイン パスワード（**password** コマンドで設定）を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスで Telnet ユーザまたは SSH ユーザを認証する前に、**telnet** コマンドまたは **ssh** コマンドを使用してセキュリティ アプライアンスへのアクセスを設定する必要があります。これらのコマンドでは、セキュリティ アプライアンスとの通信を許可する IP アドレスを指定します。

セキュリティ アプライアンスへのログイン

セキュリティ アプライアンスに接続した後、ログインしてユーザ EXEC モードにアクセスします。

- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。SSH の場合、ユーザ名に「pix」と入力し、ログイン パスワードを入力します。
- このコマンドを使用して Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。

特権 EXEC モードへのアクセス

特権 EXEC モードを開始するには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースのみを使用している場合）。

- enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- enable 認証を設定している場合、セキュリティ アプライアンスによってユーザ名とパスワードの入力が求められます。

ローカル データベースを使用する認証の場合、**login** コマンドを使用できます。このコマンドでは、ユーザ名は維持されますが、認証をオンにするコンフィギュレーションは必要ありません。

ASDM へのアクセス

デフォルトでは、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワードを使用して ASDM にログインできます。ただし、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされます。

このコマンドを使用して HTTPS 認証を設定し、ローカル データベースを指定できますが、その機能はデフォルトで常にイネーブルです。AAA サーバを認証に使用する場合、設定する必要があるのは HTTPS 認証のみです。HTTPS 認証では AAA サーバ グループ用の SDI プロトコルがサポートされません。HTTPS 認証のユーザ名プロンプトの最大長は 30 文字です。パスワードの最大長は 16 文字です。

システム実行スペースでの AAA コマンドのサポートなし

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。

許可されるログイン試行の回数

次の表に示すように、**aaa authentication console** コマンドで選択するオプションによって、セキュリティ アプライアンス CLI への認証されたアクセスに対するプロンプトのアクションは異なります。

オプション	許可されるログイン試行の回数
enable	3 回失敗するとアクセスが拒否される。
serial	成功するまで何回も試行できる。
ssh	3 回失敗するとアクセスが拒否される。
telnet	成功するまで何回も試行できる。
http	成功するまで何回も試行できる。

ユーザ CLI および ASDM アクセスの制限

aaa authorization exec authentication-server コマンドを使用して管理認可を設定し、ローカル ユーザ、RADIUS、TACACS+、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を、CLI、ASDM、または **enable** コマンドへのアクセスを制限できます。

（注） シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** を設定している場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- RADIUS または LDAP（マッピングされた）ユーザ：次の値のいずれかについて、Service-Type 属性を設定します （LDAP 属性をマッピングするには、**ldap attribute-map** コマンドを参照してください）。
  - Service-Type 6（管理）：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）：**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - Service-Type 5（発信）：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPSec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。
- TACACS+ ユーザ：「service=shell」で認可が要求され、サーバは PASS または FAIL で応答します。
  - PASS、特権レベル 1：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - PASS、特権レベル 2 以上：**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。
- ローカル ユーザ：**service-type** コマンドを設定します。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で、**aaa authentication console** コマンドを使用する例を示します。

```
hostname(config)# aaa authentication telnet console radius
```

次に、サーバ グループ「AuthIn」をイネーブル認証用に指定する例を示します。

```
hostname(config)# aaa authentication enable console AuthIn
```

次に、**aaa authentication console** コマンドを使用して、グループ「svrgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックさせる例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザ認証に使用する AAA サーバを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。

ldap map-attributes	LDAP 属性を、セキュリティ アプライアンスで認識できる RADIUS 属性にマッピングします。
service-type	ローカル ユーザの CLI アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication include, exclude

セキュリティ アプライアンスを経由する接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication include** コマンドを使用します。認証からアドレスを除外するには、**aaa authentication exclude** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを認証から除外します。
include	認証が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認証が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[-*port*] • **udp**/*port*[-*port*] • **icmp**/*type* • *protocol*[/*port*[-*port*]] プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

アクセス リストで指定されているトラフィックの認証をイネーブルにするには、**aaa authentication match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authentication include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authentication match** コマンドを使用する必要があります。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については **timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」ストリングをキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスを *すべて* 終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- ポート 443 は HTTPS 用

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、セキュリティ アプライアンスにより元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（注）　**aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信して、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL でセキュリティ アプライアンスの直接認証を受けることができます。

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを表示します。

例

次に、外部インターフェイスで TCP トラフィックを認証に含める例を示します。内部 IP アドレス 192.168.0.0 およびネットマスク 255.255.0.0、すべてのホストの外部 IP アドレスを指定し、tacacs+ という名前のサーバ グループを使用します。2 番めのコマンドラインでは、外部インターフェイスで Telnet トラフィックを除外します。内部アドレス 192.168.38.0、すべてのホストの外部 IP アドレスを指定します。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

次に、*interface-name* パラメータの使用方法を示す例を示します。セキュリティ アプライアンスには、内部ネットワーク 192.168.1.0、外部ネットワーク 209.165.201.0（サブネット マスク 255.255.255.224）、および境界ネットワーク 209.165.202.128（サブネット マスク 255.255.255.224）があります。

次の例では、内部ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、内部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから内部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、境界ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

関連コマンド

コマンド	説明
aaa authentication console	管理アクセスの認証をイネーブルにします。
aaa authentication match	通過トラフィックのユーザ認証をイネーブルにします。
aaa authentication secure-http-client	HTTP 要求がセキュリティ アプライアンスを通過するのを許可する前に、セキュリティ アプライアンスに対してセキュアなユーザ認証方式を提供します。
aaa-server	グループ関連のサーバ属性を設定します。
aaa-server host	ホスト関連の属性を設定します。

aaa authentication listener

HTTP(S) リスニング ポートでネットワーク ユーザを認証できるようにするには、グローバル コンフィギュレーション モードで **aaa authentication listener** コマンドを使用します。リスニング ポートをイネーブルにすると、セキュリティ アプライアンスでは直接接続に対して、およびオプションで通過トラフィックに対して認証ページを提供します。リスナーをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

構文の説明

http[s]	リッスンするプロトコル（HTTP または HTTPS）を指定します。このコマンドは、プロトコルごとに別々に入力します。
interface_name	リスナーをイネーブルにするインターフェイスを指定します。
port *portnum*	セキュリティ アプライアンスで直接トラフィックまたはリダイレクトされたトラフィックをリッスンするポート番号を指定します。デフォルトは 80（HTTP）および 443（HTTPS）です。任意のポート番号を使用して同じ機能を保持できますが、直接認証ユーザがそのポート番号を認識している必要があります。これは、リダイレクトされたトラフィックは正しいポート番号に自動的に送信されますが、直接認証するユーザは、ポート番号を手動で指定する必要があるためです。
redirect	セキュリティ アプライアンスによって提供される認証 Web ページに通過トラフィックをリダイレクトします。このキーワードを指定しないと、セキュリティ アプライアンス インターフェイスへのトラフィックだけが認証 Web ページにアクセスできます。

デフォルト

デフォルトでは、リスナー サービスはディセーブルであり、HTTP 接続では基本 HTTP 認証が使用されます。リスナーをイネーブルにした場合、デフォルトのポートは 80（HTTP）および 443（HTTPS）です。

7.2(1) からアップグレードする場合、リスナーはポート 1080（HTTP）および 1443（HTTPS）でイネーブルになります。**redirect** オプションもイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

aaa authentication listener コマンドを使用しないと、**aaa authentication match** または **aaa authentication include** コマンドの設定後に HTTP(S) ユーザがセキュリティ アプライアンスで認証する必要があるときに、セキュリティ アプライアンスでは基本 HTTP 認証が使用されます。HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードを指定して設定すると、セキュリティ アプライアンスにより、すべての HTTP(S) 認証要求はセキュリティ アプライアンスによって提供される Web ページにリダイレクトされます。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

aaa authentication listener コマンドを **redirect** オプションを*指定しない*で入力した場合、セキュリティ アプライアンスでの直接認証のみがイネーブルとなり、通過トラフィックでは基本 HTTP 認証が使用されます。**redirect** オプションによって、直接認証と通過トラフィック認証の両方がイネーブルになります。直接認証は、認証チャレンジをサポートしないトラフィック タイプを認証するときに役立ちます。他のサービスを使用する前に、各ユーザをセキュリティ アプライアンスで直接認証できます。

（注） **redirect** オプションをイネーブルにした場合、インターフェイスの IP アドレスを変換する同じインターフェイス、およびリスナー用に使用される同じポートに対して、スタティック PAT も設定することはできません。NAT は成功しますが、認証は失敗します。たとえば、次のコンフィギュレーションはサポートされません。

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside redirect
```

次のコンフィギュレーションはサポートされます。リスナーによって、ポートはデフォルトの 80 ではなく 1080 が使用されます。

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside port 1080 redirect
```

例

次に、HTTP および HTTPS 接続をデフォルトのポートにリダイレクトするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

次に、セキュリティ アプライアンスへの直接認証要求を許可する例を示します。通過トラフィックによって基本 HTTP 認証が使用されます。

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

次に、HTTP および HTTPS 接続をデフォルト以外のポートにリダイレクトするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

関連コマンド

コマンド	説明
aaa authentication match	通過トラフィックのユーザ認証を設定します。
aaa authentication secure-http-client	SSL をイネーブルにし、HTTP クライアントとセキュリティ アプライアンスの間のユーザ名とパスワードのセキュアな交換をイネーブルにします。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。
virtual http	基本 HTTP 認証による HTTP 認証のカスケードをサポートします。

aaa authentication match

セキュリティ アプライアンス を通じた接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication match** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

構文の説明

acl_name	拡張アクセス リストの名前を指定します。
interface_name	ユーザを認証するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authentication match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります （タイムアウト値については **timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」ストリングをキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスを *すべて*終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- HTTPS の場合はポート 443（**aaa authentication listener** コマンドが必要）

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、セキュリティ アプライアンスにより元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（注）　**aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信して、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL でセキュリティ アプライアンスの直接認証を受けることができます。

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを表示します。

例

次に、**aaa authentication match** コマンドを使用する例を示します。

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

このコンテキストでは、次のコマンドは

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

次のコマンドと同じです。

```
hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa コマンド ステートメントのリストでは、**access-list** コマンド ステートメント間の順序に依存します。たとえば、次のコマンドを入力します。

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

その後で、次のコマンドを入力します。

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

セキュリティ アプライアンスは、まず **mylist** 内の **access-list** コマンド ステートメント グループに一致があるか確かめ、次に **yourlist** 内の **access-list** コマンド ステートメント グループに一致があるかを確かめます。

関連コマンド

コマンド	説明
aaa authorization	ユーザ認可サービスをイネーブルにします。
access-list extended	アクセス リストを作成します。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication secure-http-client

SSL をイネーブルにし、HTTP クライアントとセキュリティ アプライアンスの間のユーザ名とパスワードのセキュアな交換をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication secure-http-client** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**aaa authentication secure-http-client** コマンドによって、ユーザの HTTP ベース Web 要求がセキュリティ アプライアンスを通過するのを許可する前に、セキュリティ アプライアンスに対するセキュアなユーザ認証方式が提供されます。

aaa authentication secure-http-client

no aaa authentication secure-http-client

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authentication secure-http-client コマンドによって、（SSL を介して）HTTP クライアント認証が保護されます。このコマンドは、HTTP カットスルー プロキシ認証用に使用されます。

aaa authentication secure-http-client コマンドには、次の制限があります。

- 実行時に、最大で 16 個の HTTPS 認証プロセスが許可されます。16 個の HTTPS 認証プロセスすべてが実行されている場合、認証を必要とする 17 番めの新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されると（**uauth timeout** が 0 に設定される）、HTTPS 認証は機能しない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この状況を回避するには、**timeout uauth 0:0:1** コマンドで **uauth timeout** を 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。
- HTTPS 認証は SSL ポート 443 で行われるため、HTTP クライアントから HTTP サーバ ポート 443 へのトラフィックをブロックするように、**access-list** コマンド ステートメントを設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、

SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、最初の行でスタティック PAT が Web トラフィックに対して設定されるため、HTTPS 認証コンフィギュレーションをサポートするために 2 番めの行を追加する必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

例

次に、HTTP トラフィックがセキュアに認証されるように設定する例を示します。

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

「...」は、*authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag* の値を表します。

次に、HTTPS トラフィックがセキュアに認証されるように設定するコマンドを示します。

```
hostname (config)# aaa authentication include https...
```

「...」は、*authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* の値を表します。

（注） **aaa authentication secure-https-client** コマンドは、HTTPS トラフィックには必要ありません。

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブルにします。
virtual telnet	セキュリティ アプライアンス仮想サーバにアクセスします。

aaa authorization command

aaa authorization command コマンドでは、CLI でのコマンド実行が認可の対象かどうかを指定します。コマンド認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization command** コマンドを使用します。コマンド認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization command {LOCAL | *tacacs+ server_tag* **[LOCAL]}**

no aaa authorization command {**LOCAL |** *tacacs+ server_tag* **[LOCAL]}**

構文の説明

LOCAL	**privilege** コマンドによって設定されるローカル コマンド特権レベルをイネーブルにします。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、セキュリティ アプライアンスはそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。 TACACS+ サーバ グループ タグの後に **LOCAL** を指定した場合、TACACS+ サーバ グループが使用できないときにフォールバックとしてのみ、ローカル ユーザ データベースがコマンド認可に使用されます。
tacacs+ server_tag	TACACS+ 認可サーバの定義済みのサーバ グループ タグを指定します。**aaa-server** コマンドで定義した AAA サーバ グループ タグです。

デフォルト

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	TACACS+ サーバ グループが一時的に使用できないときの LOCAL 認可へのフォールバックのサポートが追加されました。
8.0(2)	RADIUS サーバまたは LDAP サーバで定義される特権レベルのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。コマンドへのアクセスを制御する場合には、セキュリティ アプライアンス にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：セキュリティ アプライアンスでコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、セキュリティ アプライアンスはそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザが存在しなくても、また CLI 認証や enable 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、セキュリティ アプライアンスによってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、セキュリティ アプライアンスによってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド認可をオンにしない限り使用されません （詳細については、**enable** コマンドを参照してください）。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバでチェックされます。

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。これにより、異なるセキュリティ コンテキストに対して異なるコマンド認可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの認可が前のコンテキスト セッションでのユーザの認可と異なる場合に、混乱が生じる可能性があります。

  これは、発行される各コマンドを特定の管理者に正確に関連付けることができる場合に限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドの使用が許可されているすべての管理者は enable_15 ユーザ名を他のコンテキストで使用できるため、enable_15 ユーザ名で

ログインしたユーザをコマンド アカウンティング レコードで簡単に特定できるとは限りません。コンテキストごとに異なるアカウンティング サーバを使用する場合は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

コマンド許可を設定する場合は、次の点を考慮します。

- **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
- コンテキストごとに別々にコマンドを認可する場合は、**changeto** コマンドの使用許可を持つ管理者に対しても拒否されるコマンドが enable_15 ユーザ名でも拒否されることを、各コンテキストで確認してください。

セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

（注） システム実行スペースでは **aaa** コマンドはサポートされません。したがって、システム実行スペースではコマンド認可は使用できません。

ローカル コマンド認可の前提条件

- **aaa authentication enable console** コマンドを使用して、ローカル、RADIUS、または LDAP 認証の enable 認証を設定します。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を維持するために必要です。

  または、コンフィギュレーションが不要な **login** コマンド（認証を伴う **enable** コマンドと同じ）を使用できます。enable 認証ほどセキュアではないため、このオプションは推奨しません。

  CLI 認証（**aaa authentication** {**ssh** | **telnet** | **serial**} **console**）を使用することもできますが、必須ではありません。

- RADIUS が認証に使用されている場合、**aaa authorization exec authentication-server** コマンドを使用して、RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにすることができますが、必須ではありません。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可もイネーブルにします。このコマンドを使用すると、ローカル コマンド許可に影響するかも知れません。**authentication-server** キーワードを使用すると、ユーザの認証に使用されたサーバから特権レベルを取得するデフォルトの動作を維持します（LDAP（マッピング済み）、LOCAL および RADIUS サーバに適用されます）。ただし、このオプションは、TACACS+ サーバからのユーザ特権レベルの取得をイネーブルにします。
- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：**username** コマンドを使用して、ローカル データベース内のユーザを特権レベル 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。
- コマンド特権レベルの設定については、**privilege** コマンドを参照してください。

TACACS+ コマンド認可

TACACS+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力する場合、セキュリティ アプライアンスによってコマンドとユーザ名が TACACS+ サーバに送信され、コマンドが認可されているかどうかが判別されます。

TACACS+ サーバによるコマンド認可を設定するときは、意図したとおりに機能することが確認できるまで、コンフィギュレーションを保存しないでください。間違いによりロック アウトされた場合、通常はセキュリティ アプライアンスを再起動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムとセキュリティ アプライアンスへの完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合、ローカル ユーザおよびコマンド特権レベルを設定する必要があります。

TACACS+ サーバの設定については、『*Cisco ASA 5500 Series Command Line Configuration Guide*』を参照してください。

TACACS+ コマンド認可の前提条件

- **aaa authentication** {**ssh** | **telnet** | **serial**} **console** コマンドを使用して、CLI 認証を設定します。
- **aaa authentication enable console** コマンドを使用して、**enable** 認証を設定します。

例

次に、tplus1 という名前の TACACS+ サーバ グループを使用してコマンド認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization command tplus1
```

次に、tplus1 サーバ グループ内のすべてのサーバが使用できない場合に、ローカル ユーザ データベースへのフォールバックをサポートする管理認可を設定する例を示します。

```
hostname(config)# aaa authorization command tplus1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	CLI、ASDM、および enable 認証をイネーブルにします。
aaa authorization exec authentication-server	RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにします。
aaa-server host	ホスト関連の属性を設定します。
aaa-server	グループ関連のサーバ属性を設定します。
enable	特権 EXEC モードを開始します。
ldap map-attributes	LDAP 属性を、セキュリティ アプライアンスで使用できる RADIUS 属性にマッピングします。
login	ローカル データベースを認証に使用して特権 EXEC モードを開始します。
service-type	ローカル データベース ユーザの CLI、ASDM、およびイネーブル アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization exec authentication-server

管理認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization exec authentication-server** コマンドまたは **aaa authorization exec** コマンドを使用します。管理許可をディセーブルにするには、**aaa authorization exec authentication-server** コマンドの **no** 形式または、**no aaa authorization exec** コマンドを使用します。

aaa authorization exec [authentication-server]

no aaa authorization exec [authentication-server]

構文の説明

authentication-server	ユーザの認証に使用されたサーバから認可属性が取得されることを指定します。

デフォルト

デフォルトでは、このコマンドはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

aaa authorization exec authentication-server コマンドを使用すると、ユーザの service-type クレデンシャルはコンソール アクセスの許可の前に検査されます。

no aaa authorization exec authentication-server コマンドを使用するときは、以下に注意してください：

- コンソール アクセスの許可の前に、ユーザの service-type クレデンシャルはチェックされません。
- コマンド認可が設定されている場合、RADIUS、LDAP、および TACACS+ ユーザについて AAA サーバで特権レベル属性が見つかると、特権レベル属性が引き続き適用されます。

ユーザが CLI、ASDM、または **enable** コマンドにアクセスするときにユーザを認証するように **aaa authentication console** コマンドを設定すると、ユーザ コンフィギュレーションに応じて **aaa authorization exec authentication-server** コマンドで管理アクセスを制限できます。

（注） シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** を設定している場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- LDAP マッピング済みユーザ : LDAP 属性をマッピングするには、**ldap attribute-map** コマンドを参照してください。
- RADIUS ユーザ : 次の値のいずれかにマッピングする IETF RADIUS numeric **service-type** 属性を使用します。
  - Service-Type 5（発信）は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。
  - Service-Type 6（管理）は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）は、**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。

（注） 認識される service-type は、ログイン（1）、フレーム化（2）、管理（6）、および NAS プロンプト（7）のみです。その他の service-type を使用すると、アクセスは拒否されます。

- TACACS+ ユーザ :「service=shell」エントリで許可を要求し、サーバは次のように PASS または FAIL で応答します。
  - PASS、特権レベル 1 は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - PASS、特権レベル 2 以上は、**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。
- ローカル ユーザ : **service-type** コマンドを設定します。これは、**username** コマンドのユーザ名コンフィギュレーション モードです。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で、**aaa authentication console** コマンドを使用する例を示します。

```
hostname(config)# aaa authentication telnet console radius
```

次に、サーバ グループ「AuthIn」をイネーブル認証用に指定する例を示します。

```
hostname(config)# aaa authentication enable console AuthIn
```

次に、**aaa authentication console** コマンドを使用して、グループ「svrgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックさせる例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	コンソール認証をイネーブルにします。
ldap attribute-map	LDAP 属性をマッピングします。
service-type	ローカル ユーザの制限 CLI アクセス。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization include, exclude

セキュリティ アプライアンス を介した接続の許可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization include** コマンドを使用します。許可からアドレスを除外するには、**aaa authorization exclude** コマンドを使用します。許可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを許可から除外します。
include	認可が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認可を要求するインターフェイスの名前を指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認可が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[**-***port*] • **udp**/*port*[**-***port*] • **icmp**/*type* • *protocol*[/*port*[**-***port*]] **（注）** ポート範囲を指定すると、予期できない結果が許可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを許可する場合もありますが、範囲が受け入れられると、このような許可は行われません。

デフォルト

IP アドレス **0** は「すべてのホスト」を意味します。ローカル IP アドレスを **0** に設定すると、許可されるホストを許可サーバによって決定できます。

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**exclude** パラメータによって、特定のホストに対して除外するポートをユーザが指定できるようになりました。

使用上のガイドライン

アクセス リストで指定されているトラフィックの認可をイネーブルにするには、**aaa authorization match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authorization include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authorization match** コマンドを使用する必要があります。

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

IP アドレスごとに 1 つの **aaa authorization include** コマンドが許可されます。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

（注） ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、TACACS+ プロトコルを使用する例を示します。

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication ssh console tplus1
```

この例では、最初のコマンド ステートメントで tplus1 という名前のサーバ グループを作成し、このグループで使用する TACACS+ プロトコルを指定しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 3 つのコマンド ステートメントで指定しているのは、外部インターフェイス経由で外部ホストへの接続を開始するすべてのユーザを tplus1 サーバ グループを使用して認証すること、正常に認証されたユーザに対してはすべてのサービスの使用を認可すること、および

すべての発信接続情報をアカウンティング データベースに記録することです。最後のコマンド ステートメントでは、セキュリティ アプライアンスのコンソールへの SSH アクセスには、tplus1 サーバ グループからの認証が必要であることを指定しています。

次に、外部インターフェイスからの DNS ルックアップに対する認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

次に、内部ホストから内部インターフェイスに到着する ICMP echo-reply パケットの認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

これは、ユーザが Telnet、HTTP、または FTP を使用して認証されていない場合は外部ホストを ping できないことを意味します。

次に、内部ホストから内部インターフェイスに到着する ICMP エコー（ping）についてのみ認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

関連コマンド

コマンド	説明
aaa authorization command	コマンドの実行が認可の対象かどうかを指定します。または、指定したサーバ グループ内のすべてのサーバがディセーブルである場合に、ローカル ユーザ データベースへのフォールバックをサポートするように管理認可を設定します。
aaa authorization match	特定の access-list コマンド名に対して LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization match

セキュリティ アプライアンス を通じた接続の許可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization match** マンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

構文の説明

acl_name	拡張アクセス リストの名前を指定します。**access-list extended** コマンドを参照してください。**許可** ACE は、一致したトラフィックを認可するようにマークします。一方、**拒否**エントリは、一致したトラフィックを認可から除外します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authorization match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。**aaa authorization match** コマンドによる RADIUS 認可では、FWSM への VPN 管理接続の認可のみがサポートされます。

認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

（注） ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、**aaa** コマンドで tplus1 サーバ グループを使用する例を示します。

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization match myacl inside tplus1
```

この例では、最初のコマンド ステートメントで tplus1 サーバ グループを TACACS+ グループとして定義しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 2 つのコマンド ステートメントでは、内部インターフェイスを通過する、任意の外部ホストへの接続が tplus1 サーバ グループを使用して認証され、これらのすべての接続がアカウンティング データベースに記録されることを指定しています。最後のコマンド ステートメントでは、myacl 内の ACE に一致する接続が tplus1 サーバ グループ内の AAA サーバによって認可されることを指定しています。

関連コマンド

コマンド	説明
aaa authorization	ユーザ認可をイネーブルまたはディセーブルにします。
clear configure aaa	すべての aaa コンフィギュレーション パラメータをデフォルト値にリセットします。
clear uauth	1 人のユーザまたはすべてのユーザについて、AAA 認可キャッシュと AAA 認証キャッシュを削除します。これにより、次に接続を作成するときにユーザは再認証する必要があります。
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および認可のために認可サーバに提供されたユーザ名、ユーザ名がバインドされている IP アドレス、およびユーザは認証されただけかキャッシュされたサービスを持っているかを表示します。

aaa local authentication attempts max-fail

セキュリティ アプライアンス で特定のユーザ アカウントに対して許可されるローカル ログイン試行の連続失敗回数を制限するには（特権レベル 15 のユーザを除きます。この機能はレベル 15 のユーザには影響しません）、グローバル コンフィギュレーション モードで **aaa local authentication attempts max-fail** コマンドを使用します。このコマンドは、ローカル ユーザ データベースによる認証だけに影響します。この機能をディセーブルにし、ローカル ログイン試行の連続失敗回数を無制限に許可するには、このコマンドの **no** 形式を使用します。

aaa local authentication attempts max-fail *number*

構文の説明

number	ユーザがロック アウトされるまでに間違ったパスワードを入力できる最大回数。この数の範囲は、1 ～ 16 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを省略すると、ユーザが間違ったパスワードを入力できる回数に制限は設けられません。

間違ったパスワードを入力した試行回数が設定回数に達すると、ユーザはロック アウトされ、管理者がユーザ名をアンロックするまで、ユーザは正常にログインできません。ユーザ名のロックまたはアンロックにより、システム ログ メッセージが生成されます。

特権レベル 15 のユーザはこのコマンドの影響を受けず、ロック アウトされることはありません。

ユーザが正常に認証されるか、セキュリティ アプライアンスがリブートされると、失敗試行回数は 0 にリセットされ、ロックアウト ステータスは No にリセットされます。

例

次に、**aaa local authentication attempts max-limits** コマンドを使用して、許可される失敗試行の最大回数を 2 に設定する例を示します。

```
hostname(config)# aaa local authentication attempts max-limits 2
hostname(config)#
```

関連コマンド

コマンド	説明
clear aaa local user lockout	指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更しないで、ユーザ認証失敗試行回数をリセットします。
show aaa local user	現在ロックされているユーザ名のリストを表示します。

aaa mac-exempt

認証および認可から免除する MAC アドレスの定義済みリストの使用を指定するには、グローバル コンフィギュレーション モードで **aaa mac-exempt** コマンドを使用します。追加できる **aaa mac-exempt** コマンドは 1 つだけです。MAC アドレスのリストの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

構文の説明

id	**mac-list** コマンドで設定した MAC リスト番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa mac-exempt コマンドを使用する前に、**mac-list** コマンドを使用して MAC リスト番号を設定します。MAC リスト内の permit エントリによって MAC アドレスは認証および認可から免除され、deny エントリによって MAC アドレスの認証および認可が要求されます（認証および認可がイネーブルの場合）。追加できる **aaa mac-exempt** コマンドのインスタンスは 1 つだけであるため、免除するすべての MAC アドレスを MAC リストに含めてください。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次に、00a0.c95d.02b2 を除く MAC アドレスのグループの認証をバイパスする例を示します。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
```

```
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。
mac-list	認証および認可から MAC アドレスを免除するために使用する MAC アドレスのリストを指定します。

aaa proxy-limit

ユーザごとに許可される同時プロキシ接続の最大数を設定することで、uauth セッションの制限を手動で設定するには、グローバル コンフィギュレーション モードで **aaa proxy-limit** コマンドを使用します。プロキシをディセーブルにするには、**disable** パラメータを使用します。デフォルトのプロキシ制限値（16）に戻すには、このコマンドの **no** 形式を使用します。

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

構文の説明

disable	プロキシは許可されません。
proxy_limit	ユーザごとに許可される同時プロキシ接続数（1 ～ 128）を指定します。

デフォルト

デフォルトのプロキシ制限値は 16 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

送信元アドレスがプロキシ サーバである場合は、この IP アドレスを認証から除外するか、許容される未処理 AAA 要求の数を増やすことを検討してください。

例

次に、ユーザごとに許可される未処理認証要求の最大数を設定する例を示します。

```
hostname(config)# aaa proxy-limit 6
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、あるいは ASDM ユーザ認証をイネーブルまたはディセーブルにするか、表示します。
aaa authorization	LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。

aaa-server host	AAA サーバを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa-server

AAA サーバ グループを作成し、すべてのグループ ホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server** コマンドを使用します。指定したグループを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

構文の説明

server-tag	サーバ グループ名を指定します。**aaa-server host** コマンドで指定した名前と同じにします。他の AAA コマンドで、この AAA サーバ グループ名を参照します。
protocol *server-protocol*	グループ内のサーバによってサポートされる AAA プロトコルを指定します。 • **http-form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	http-form プロトコルが追加されました。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループ プロトコルを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。

シングル モードで最大 15 個のサーバ グループ、マルチ モードでコンテキストごとに 4 個のサーバ グループを保持できます。各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

例

次に、**aaa-server** コマンドを使用して、TACACS+ サーバ グループ コンフィギュレーションの詳細を変更する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
```

関連コマンド

コマンド	説明
accounting-mode	アカウンティング メッセージが単一のサーバに送信されるか（シングル モード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定します。
reactivation-mode	障害の発生したサーバを再度アクティブにする方式を指定します。
max-failed-attempts	サーバ グループ内の所定のサーバが非アクティブ化されるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server active/fail

障害とマークされた AAA サーバを再度アクティブにするには、特権 EXEC モードで **aaa-server active** コマンドを使用します。アクティブなサーバを障害状態にするには、特権 EXEC モードで **aaa-server fail** コマンドを使用します。

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

構文の説明

active	サーバをアクティブ状態に設定します。
fail	サーバを障害状態に設定します。
host	ホストの IP アドレス名または IP アドレスを指定します。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server_ip	AAA サーバの IP アドレスを指定します。
server_tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用しないと、グループ内の障害が発生したサーバは、グループ内のすべてのサーバに障害が発生するまで障害状態のままになります。グループ内のすべてのサーバに障害が発生した後に、サーバはすべて再度アクティブにされます。

例

次に、サーバ 192.168.125.60 の状態を表示し、手動で再度アクティブにする例を示します。

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
hostname# aaa-server active host 192.168.125.60
```

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server host

AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト コンフィギュレーション モードが開始されます。このモードから、ホスト固有の AAA サーバ接続データを指定および管理できます。ホスト コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

構文の説明

(*interface-name***)**	（任意）認証サーバが配置されているネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。インターフェイスを指定しない場合、デフォルトは **inside** です（使用可能な場合）。
key	（任意）127 文字までの大文字と小文字が区別される英数字のキーワードを指定します。RADIUS サーバまたは TACACS+ サーバ上のキーと同じ値です。127 文字を超えて入力された文字があれば無視されます。このキーは、セキュリティ アプライアンスとサーバの間でデータを暗号化するために使用されます。このキーは、セキュリティ アプライアンスとサーバ システムの両方で同じである必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。ホスト モードで **key** コマンドを使用して、キーを追加または変更できます。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server-ip	AAA サーバの IP アドレスを指定します。
server-tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。
timeout *seconds*	（任意）要求のタイムアウト間隔。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。ホスト モードで **timeout** コマンドを使用して、タイムアウト間隔を変更できます。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

デフォルトのインターフェイスは、inside です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	DNS 名のサポートが追加されました。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。

シングル モードで最大 15 個のサーバ グループ、マルチ モードでコンテキストごとに 4 個のサーバ グループを保持できます。各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

aaa-server host コマンドを入力した後、ホスト固有のパラメータを設定できます。

例

次に、「watchdogs」という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、そのサーバの Kerberos レルムを定義する例を示します。

（注） Kerberos 領域名では数字と大文字だけを使用します。セキュリティ アプライアンスは領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

次に、「svrgrp1」という名前の SDI AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、タイムアウト間隔を 6 秒に、リトライ間隔を 7 秒に、SDI バージョンをバージョン 5 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

absolute

時間範囲が有効である場合に絶対時間を定義するには、時間範囲コンフィギュレーション モードで **absolute** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

absolute [**end** *time date*] [**start** *time date*]

no absolute

構文の説明

date	日付を day month year 形式で指定します（たとえば、1 January 2006）。年の有効な範囲は、1993 ～ 2035 です。
time	時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。

デフォルト

開始時刻および日付を指定しない場合、permit ステートメントまたは deny ステートメントはただちに有効になり、常にオンです。同様に、最大終了時刻は 23:59 31 December 2035 です。終了時刻および日付を指定しない場合、関連付けられている permit ステートメントまたは deny ステートメントは無期限に有効です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

例

次に、ACL を 2006 年 1 月 1 日の午前 8 時にアクティブにする例を示します。例を示します。

```
hostname(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

関連コマンド

コマンド	説明
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

accept-subordinates

デバイスにインストールされていない下位 CA 証明書がフェーズ 1 の IKE 交換で提供されたときに、その証明書を受け入れるようにセキュリティ アプライアンスを設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **accept-subordinates** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

accept-subordinates

no accept-subordinates

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定はオンです（下位証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェーズ 1 の処理中に、IKE ピアによって下位証明書とアイデンティティ証明書の両方が渡される場合があります。下位証明書はセキュリティ アプライアンスにインストールされない場合があります。このコマンドを使用すると、管理者はデバイス上にトラストポイントとして設定されていない下位 CA 証明書をサポートできます。確立されたすべてのトラストポイントのすべての下位 CA 証明書が受け入れ可能である必要はありません。つまり、このコマンドを使用すると、デバイスで、証明書チェーン全体をローカルにインストールすることなく、その証明書チェーンを認証できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、セキュリティ アプライアンスでトラストポイント central の下位証明書を受け入れることができるようにする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

access-group

アクセス リストをインターフェイスにバインドするには、グローバル コンフィギュレーション モードで **access-group** コマンドを使用します。アクセス リストをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

access-group *access-list* {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**]

no access-group *access-list* {**in** | **out**} **interface** *interface_name*

構文の説明

access-list	アクセス リストの *ID*。
control-plane	（任意）ルールが to-the-box トラフィック用かどうかを指定します。
in	指定したインターフェイスで着信パケットをフィルタリングします。
interface *interface-name*	ネットワーク インターフェイスの名前。
out	指定したインターフェイスで発信パケットをフィルタリングします。
per-user-override	（任意）ダウンロード可能なユーザ アクセス リストが、インターフェイスに適用されているアクセス リストを上書きできるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

access-group コマンドは、アクセス リストをインターフェイスにバインドします。アクセス リストは、インターフェイスへの着信トラフィックに適用されます。**access-list** コマンド ステートメントで **permit** オプションを入力すると、セキュリティ アプライアンスによってパケットの処理は続行されます。**access-list** コマンド ステートメントで **deny** オプションを入力すると、セキュリティ アプライアンスによってパケットは廃棄され、次の syslog メッセージが生成されます。

```
%hostname-4-106019: IP packet from source_addr to destination_addr, protocol
protocol received from interface interface_name deny by access-group id
```

per-user-override オプションを指定すると、ダウンロードしたアクセス リストで、インターフェイスに適用されているアクセス リストを上書きできます。オプションの *per-user-override* 引数がないと、セキュリティ アプライアンスによって既存のフィルタリング動作が保持されます。*per-user-override* があると、セキュリティ アプライアンスにより、ユーザに関連付けられているユーザごとのアクセス

リスト（ダウンロードされた場合）の **permit** または **deny** ステータスで、**access-group** コマンドに関連付けられているアクセス リストの permit または deny ステータスを上書きできるようになります。さらに、次のルールが適用されます。

- パケットが到着した時点で、そのパケットに関連付けられているユーザごとのアクセス リストがない場合、インターフェイス アクセス リストが適用されます。
- ユーザごとのアクセス リストは、**timeout** コマンドの **uauth** オプションで指定されたタイムアウト値によって管理されますが、このタイムアウト値は、ユーザごとの AAA セッション タイムアウト値によって上書きできます。
- 既存のアクセス リスト ログ動作は同じです。たとえば、ユーザごとのアクセス リストのためにユーザ トラフィックが拒否された場合、syslog メッセージ 109025 が記録されます。ユーザ トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとのアクセス リストのログ オプションは、影響を及ぼしません。

access-list コマンドは常に **access-group** コマンドとともに使用します。

access-group コマンドは、アクセス リストをインターフェイスにバインドします。**in** キーワードによって、アクセス リストは指定したインターフェイス上のトラフィックに適用されます。**out** キーワードによって、アクセス リストは発信トラフィックに適用されます。

（注）　1 つ以上の **access-group** コマンドによって参照されるアクセス リストから、すべての機能エントリ（permit ステートメントおよび deny ステートメント）を削除すると、**access-group** コマンドはコンフィギュレーションから自動的に削除されます。**access-group** コマンドは、空のアクセス リストまたはコメントだけを含むアクセス リストを参照できません。

no access-group コマンドは、アクセス リストをインターフェイス *interface_name* からアンバインドします。

show running config access-group コマンドは、インターフェイスにバインドされている現在のアクセス リストを表示します。

clear configure access-group コマンドは、インターフェイスからすべてのアクセス リストを削除します。

（注）　to-the-box 管理トラフィック用のアクセス コントロール ルール（**http**、**ssh**、**telnet** などのコマンドで定義）は、**control-plane** オプションで適用されるアクセス リストよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box アクセス リストで明示的に拒否されている場合でも着信が許可されます。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# static (inside,outside) 209.165.201.3 10.1.1.3
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

static コマンドでは、10.1.1.3 にある Web サーバにグローバル アドレス 209.165.201.3 を指定しています。**access-list** コマンドでは、任意のホストからポート 80 を使用してグローバル アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。
show running-config access-group	コンテキスト グループのメンバーを表示します。

access-list alert-interval

拒否フローの最大数メッセージの時間間隔を指定するには、グローバル コンフィギュレーション モードで **access-list alert-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list alert-interval *secs*

no access-list alert-interval

構文の説明

secs	拒否フローの最大数メッセージの生成の時間間隔。有効な値は、1 ～ 3600 秒です。デフォルト値は 300 秒です。

デフォルト

デフォルトは 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

access-list alert-interval コマンドでは、システム ログ メッセージ 106001 を生成する時間間隔を設定します。システム ログ メッセージ 106001 によって、セキュリティ アプライアンスが拒否フローの最大数に達したことが警告されます。拒否フローの最大数に達したときに、前回のシステム ログ メッセージ 106001 が生成されてから *secs* 秒以上経過していた場合は、さらに 106001 メッセージが生成されます。

拒否フローの最大数メッセージの生成については、**access-list deny-flow-max** コマンドを参照してください。

例

次に、拒否フローの最大数メッセージの時間間隔を指定する例を示します。

```
hostname(config)# access-list alert-interval 30
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。

access-list deny-flow-max

作成できる同時拒否フローの最大数を指定するには、グローバル コンフィギュレーション モードで **access-list deny-flow-max** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list deny-flow-max

no access-list deny-flow-max

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトは、4096 個の同時拒否フローです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスが ACL 拒否フローの最大数 *n* に達すると、システム ログ メッセージ 106101 が生成されます。

例

次に、作成できる同時拒否フローの最大数を指定する例を示します。

```
hostname(config)# access-list deny-flow-max 256
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list ethertype

EtherType に基づいてトラフィックを制御するアクセス リストを設定するには、グローバル コンフィギュレーション モードで **access-list ethertype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

構文の説明

any	すべての対象へのアクセスを指定します。
bpdu	ブリッジ プロトコル データ ユニットへのアクセスを指定します。デフォルトでは、BPDU は拒否されます。
deny	条件に一致する場合、アクセスを拒否します。
hex_number	EtherType を示す 0x600 以上の 16 ビットの 16 進数値を指定します。
id	アクセス リストの名前または番号をリストします。
ipx	IPX へのアクセスを指定します。
mpls-multicast	MPLS マルチキャストへのアクセスを指定します。
mpls-unicast	MPLS ユニキャストへのアクセスを指定します。
permit	条件が一致した場合にアクセスを許可します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

log オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトの重大度レベルは 6（情報）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、16 ビットの 16 進数値で示された任意の EtherType を制御できます。EtherType ACL によってイーサネット V2 フレームがサポートされます。802.3 形式のフレームは、タイプ フィールドではなく長さフィールドを使用するため、ACL によって処理されません。ブリッジ プロトコル データ ユニットは唯一の例外であり、ACL によって処理されます。ブリッジ プロトコル データ ユニットは SNAP 方式でカプセル化されており、セキュリティ アプライアンスは特に BPDU を処理するように設計されています。

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる場合は、両方のインターフェイスに ACL を適用する必要があります。

MPLS を許可する場合は、セキュリティ アプライアンスに接続されている両方の MPLS ルータが LDP セッションまたは TDP セッション用のルータ ID としてセキュリティ アプライアンス インターフェイス上の IP アドレスを使用するように設定することにより、LDP TCP 接続と TDP TCP 接続がセキュリティ アプライアンス経由で確立されるようにします（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）の ACL を 1 つだけ適用できます。同じ ACL を複数のインターフェイスに適用することもできます。

（注） EtherType アクセス リストが **deny all** コマンドで設定されている場合、すべてのイーサネット フレームが廃棄されます。その場合でも、オートネゴシエーションなどの物理プロトコル トラフィックだけは許可されます。

例

次に、EtherType アクセス リストを追加する例を示します。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リストのカウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list extended

アクセス コントロール エントリを追加するには、グローバル コンフィギュレーション モードで **access-list extended** コマンドを使用します。アクセス リストは、同じアクセス リスト ID を持つ 1 つ以上の ACE で構成されます。アクセス リストは、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リスト全体を削除するには、**clear configure access-list** コマンドを使用します。

access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**}
{*protocol* | **object-group** *protocol_obj_grp_id*}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

no access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**} {**tcp** | **udp**}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port*] | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

構文の説明

default	（任意）ロギングをデフォルトの方式に設定します。拒否されたパケットごとにシステム ログ メッセージ 106023 を生成します。
deny	条件に合致している場合、パケットを拒否します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによってパケットはセキュリティ アプライアンスを通過できなくなります。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってトラフィックがインスペクションから免除されます。一部の機能では deny ACE の使用は許可されません（NAT など）。詳細については、アクセス リストを使用する各機能のコマンド マニュアルを参照してください。
dest_ip	パケットの送信先のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
disable	（任意）この ACE のロギングをディセーブルにします。
extended	（任意）ACE を追加します。
icmp_type	（任意）プロトコルが ICMP の場合、ICMP タイプを指定します。
id	アクセス リスト ID を最大 241 文字のストリングまたは整数として指定します。ID は、大文字と小文字が区別されます。 **ヒント** コンフィギュレーションでアクセス リスト ID を見やすくするには、すべて大文字にします。

inactive	（任意）ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。
interface *ifc_name*	インターフェイス アドレスを送信元アドレスまたは宛先アドレスとして指定します。 **（注）** トラフィックの宛先がデバイス インターフェイスである場合、アクセス リストに実際の IP アドレスを指定する代わりに interface キーワードを指定する必要があります。
interval *secs*	（任意）システム ログ メッセージ 106100 を生成するログ間隔を指定します。有効な値は、1 ～ 600 秒です。デフォルトは 300 です。
level	（任意）システム ログ メッセージ 106100 の重大度レベル（0 ～ 7）を設定します。デフォルトのレベルは 6（情報）です。
line *line-num*	（任意）ACE を挿入する行番号を指定します。行番号を指定しなかった場合は、アクセス リストの末尾に ACE が追加されます。行番号はコンフィギュレーションに保存されません。ACE の挿入場所を指定するだけです。
log	（任意）**ACE** がネットワーク アクセス（**access-group** コマンドで適用されたアクセス リスト）のパケットと一致したときのロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル（6）とデフォルト間隔（300 秒）でシステム ログ メッセージ 106100 が有効になります。**log** キーワードを入力しないと、デフォルトのシステム ログ メッセージ 106023 が生成されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。セキュリティ アプライアンスでは、ネットワーク マスク（たとえば、クラス C マスクの場合は 255.255.255.0）を使用します。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。
object-group *icmp_type_obj_grp_id*	（任意）プロトコルが ICMP の場合、ICMP タイプのオブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group icmp-type** コマンドを参照してください。
object-group *network_obj_grp_id*	ネットワーク オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group network** コマンドを参照してください。
object-group *protocol_obj_grp_id*	プロトコル オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group protocol** コマンドを参照してください。
object-group *service_obj_grp_id*	（任意）プロトコルを TCP または UDP に設定する場合、サービス オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group service** コマンドを参照してください。

operator	（任意）送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい • **neq**：等しくない • **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
permit	条件に合致している場合、パケットを許可します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによってパケットはセキュリティ アプライアンスを通過できます。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってインスペクションがパケットに適用されます。
port	（任意）プロトコルを TCP または UDP に設定する場合、TCP ポートまたは UDP ポートの番号（整数）か名前を指定します。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。
protocol	IP プロトコルの名前または番号を指定します。たとえば、UDP は 17、TCP は 6、EGP は 47 です。
src_ip	パケットの送信元のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
time-range *time_range_name*	（任意）ACE に時間範囲を適用することによって、週および 1 日の中の特定の時刻に各 ACE がアクティブになるようにスケジューリングします。時間範囲の定義については、**time-range** コマンドを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- ACE ロギングは、拒否されたパケットについてシステム ログ メッセージ 106023 を生成します。拒否されたパケットをログに記録するには、**deny ACE** が存在している必要があります。
- **log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6（情報）で、デフォルトの間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

特定のアクセス リスト名に対して入力した各 ACE は、ACE で行番号を指定しない限り、そのアクセス リストの最後に追加されます。

ACE の順序は重要です。セキュリティ アプライアンスがパケットを転送するかドロップするかを決定するとき、セキュリティ アプライアンスでは、エントリがリストされている順に、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合、残りのステートメントはチェックされません。

アクセス リストの最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除き、セキュリティ アプライアンス経由でのネットワークへのアクセスをすべてのユーザに許可する場合は、特定のアドレスを拒否し、それ以外はすべて許可する必要があります。

NAT を使用する場合、アクセス リストに対して設定する IP アドレスは、アクセス リストが付加されるインターフェイスによって異なります。インターフェイスに接続されるネットワーク上で有効なアドレスを使用する必要があります。このガイドラインは、着信アクセス グループと発信アクセス グループの両方に適用されます。使用されるアドレスは、方向ではなく、インターフェイスのみによって決まります。

TCP 接続と UDP 接続では、リターン トラフィックを許可するアクセス リストは必要ありません。これは、FWSM によって、確立された双方向接続のすべてのリターン トラフィックが許可されるためです。ただし、ICMP などのコネクションレス型のプロトコルでは、セキュリティ アプライアンスによって単方向のセッションが確立されます。そのため、両方向の ICMP を許可するアクセス リストが必要となるか（アクセス リストを送信元インターフェイスおよび宛先インターフェイスに適用）、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ICMP はコネクションレス型プロトコルであるため、両方向の ICMP を許可するアクセス リストが必要となるか（アクセス リストを送信元インターフェイスおよび宛先インターフェイスに適用）、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンでは、ICMP セッションはステートフル接続として処理されます。ping を制御するには、**echo-reply (0)**（セキュリティ アプライアンスからホストへ）または **echo (8)**（ホストからセキュリティ アプライアンスへ）を指定します。ICMP タイプのリストについては、表 1 を参照してください。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用できます。インターフェイスへのアクセス リストの適用の詳細については、**access-group** コマンドを参照してください。

（注）　アクセス リスト コンフィギュレーションを変更する場合、既存の接続がタイムアウトするのを待たずに新しいアクセス リスト情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

表 1 に、使用できる ICMP タイプの値を示します。

表 2-1　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

例

次のアクセス リストは、（アクセス リストを適用するインターフェイス上の）すべてのホストがセキュリティ アプライアンスを通過するのを許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のサンプル アクセス リストでは、192.168.1.0/24 上のホストが 209.165.201.0/27 ネットワークにアクセスすることが禁止されます。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

一部のホストのみにアクセスを制限する場合は、制限された **permit ACE** を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次のアクセス リストでは、すべてのホスト（アクセス リスト適用先のインターフェイス上にあるすべてのホスト）がアドレス 209.165.201.29 の Web サイトにアクセスすることが禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

オブジェクト グループを使用する次のアクセス リストでは、内部ネットワーク上のいくつかのホストがいくつかの Web サーバへのアクセスを禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

ネットワーク オブジェクトの 1 つのグループ（A）からネットワーク オブジェクトの別のグループ（B）へのトラフィックを許可するアクセス リストを一時的にディセーブルにするには、次のコマンドを使用します。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベースのアクセス リストを実装するには、**time-range** コマンドを使用して、1 日および週の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲をアクセス リストにバインドします。次に、「Sales」という名前のアクセス リストを「New_York_Minute」という名前の時間範囲にバインドする例を示します。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

時間範囲の定義方法の詳細については、**time-range** コマンドを参照してください。

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	ACE を番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list remark

access-list extended コマンドの前または後に追加するコメントのテキストを指定するには、グローバル コンフィギュレーション モードで **access-list remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** [*text*]

構文の説明

id	アクセス リストの名前。
line *line-num*	（任意）コメントまたは Access Control Element（ACE）を挿入する行番号。
remark text	**access-list extended** コマンドの前または後に追加するコメントのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コメント テキストには、スペース以外の文字を少なくとも 1 つ含める必要があります。空のコメントは許可されません。コメント テキストは、スペースや句読点を含め、最大 100 文字です。

コメントのみを含む ACL では **access-group** コマンドは使用できません。

例

次に、**access-list** コマンドの前または後に追加するコメントのテキストを指定する例を示します。

```
hostname(config)# access-list 77 remark checklist
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list rename

アクセス リストの名前を変更するには、グローバル コンフィギュレーション モードで **access-list rename** コマンドを使用します。

access-list *id* **rename** *new_acl_id*

構文の説明

id	既存のアクセス リストの名前。
rename *new_acl_id*	新しいアクセス リスト ID を最大 241 文字のストリングまたは整数として指定します。ID は、大文字と小文字が区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

アクセス リストを同じ名前に変更すると、コマンドは適応型セキュリティ アプライアンスによって通知なしで無視されます。

例

次に、アクセス リストの名前を TEST から OUTSIDE に変更する例を示します。

```
hostname(config)# access-list TEST rename OUTSIDE
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list standard

OSPF 再配布のルート マップで使用できる、OSPF ルートの宛先 IP アドレスを指定するアクセス リストを追加するには、グローバル コンフィギュレーション モードで **access-list standard** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

構文の説明

any	すべての対象へのアクセスを指定します。
deny	条件に一致する場合、アクセスを拒否します。
host *ip_address*	ホスト IP アドレスへのアクセスを指定します（任意）。
id	アクセス リストの名前または番号。
ip_address ip_mask	特定の IP アドレス（任意）およびサブネット マスクへのアクセスを指定します。
line *line-num*	（任意）ACE を挿入する行番号。
permit	条件が一致した場合にアクセスを許可します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-group コマンドとともに **deny** キーワード使用すると、パケットはセキュリティ アプライアンスを通過できません。デフォルトでは、特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。

送信元アドレス、ローカル アドレス、または宛先アドレスを指定するには、次のガイドラインを使用します。

- 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。
- アドレスおよびマスク 0.0.0.0 0.0.0.0 の省略形としてキーワード **any** を使用します。
- マスク 255.255.255.255 の省略形として **host** *ip_address* オプションを使用します。

例

次に、適応型セキュリティ アプライアンス経由の IP トラフィックを拒否する例を示します。

```
hostname(config)# access-list 77 standard deny
```

次に、条件に合致している場合に、適応型セキュリティ アプライアンス経由の IP トラフィックを許可する例を示します。

```
hostname(config)# access-list 77 standard permit
```

次の例は、宛先アドレスを指定する方法を示しています。

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list webtype

クライアントレス SSL VPN のフィルタリングをサポートするコンフィギュレーションにアクセス リストを追加するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

構文の説明

any	すべての IP アドレスを指定します。
any	（任意）すべての URL を指定します。
deny	条件に一致する場合、アクセスを拒否します。
host *ip_address*	ホスト IP アドレスを指定します。
id	アクセス リストの名前または番号。
interval *secs*	（任意）システム ログ メッセージ 106100 を生成する時間間隔を指定します。有効な値は、1 ～ 600 秒です。
ip_address ip_mask	特定の IP アドレスおよびサブネット マスクを指定します。
log [[**disable** | **default**] | *level*]	（任意）ACE に対してシステム ログ メッセージ 106100 が生成されることを指定します。詳細については、**log** コマンドを参照してください。
oper	*ip_address* ポートを比較します。使用できるオペランドは、lt（less than：未満）、gt（greater than：より大きい）、eq（equal：一致）、neq（not equal：不一致）、range（inclusive range：包含範囲）です。
permit	条件が一致した場合にアクセスを許可します。
port	TCP ポートまたは UDP ポートの 10 進数または名前を指定します。
time_range *name*	（任意）time-range オプションをこのアクセス リスト要素に付加するためのキーワードを指定します。
url	フィルタリングに URL を使用することを指定します。
url_string	（任意）フィルタリングする URL を指定します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。
- **log** オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトのレベルは 6（情報）です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　**access-list webtype** コマンドは、クライアントレス SSL VPN フィルタリングを設定するために使用されます。URL には、完全な URL またはファイルを除いた部分的な URL を指定できます。また、サーバのワイルドカードを含めたり、ポートを指定したりできます。

有効なプロトコル識別子は、http、https、cifs、imap4、pop3、および smtp です。URL にキーワード **any** を含めて、任意の URL を参照することもできます。アスタリスクを使用して、DNS 名のサブコンポーネントを表すことができます。

例　次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.company.com
```

次の例は、特定のファイルへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url
https://www.company.com/dir/file.html
```

次の例は、任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
show running-config access-list	適応型セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

accounting-mode

アカウンティング メッセージが単一のサーバに送信されるか（シングル モード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定するには、AAA サーバ コンフィギュレーション モードで **accounting-mode** コマンドを使用します。アカウンティング モードの指定を削除するには、このコマンドの **no** 形式を使用します。

accounting-mode {**simultaneous** | **single**}

構文の説明

simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。
single	単一のサーバにアカウンティング メッセージを送信します。

デフォルト

デフォルト値はシングル モードです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

単一のサーバにアカウンティング メッセージを送信するには、キーワード **single** を使用します。サーバ グループ内のすべてのサーバにアカウンティング メッセージを送信するには、キーワード **simultaneous** を使用します。

このコマンドは、アカウンティング（RADIUS または TACACS+）にサーバ グループが使用されている場合にのみ有効です。

例

次に、**accounting-mode** コマンドを使用して、グループ内のすべてのサーバにアカウンティング メッセージを送信する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	アカウンティング サービスをイネーブルまたはディセーブルにします。

aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始し、グループ内のすべてのホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-port

このホストの RADIUS アカウンティングに使用されるポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **accounting-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドでは、アカウンティング レコードの送信先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

accounting-port *port*

no accounting-port

構文の説明

port	RADIUS アカウンティング用のポート番号。値の範囲は 1 ～ 65535 です。

デフォルト

デフォルトでは、デバイスはアカウンティングのためにポート 1646 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS アカウンティングのデフォルトのポート番号（1646）が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティング サーバで 1646 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートに対してセキュリティ アプライアンスを設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、アカウンティング ポートを 2222 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがいずれのネットワーク サービスにアクセスしたかに関するレコードを保持します。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-server-group

アカウンティング レコード送信用の AAA サーバ グループを指定するには、さまざまなモードで **accounting-server-group** コマンドを使用します。アカウンティング サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、アカウンティングを使用して、ユーザがアクセスするネットワーク リソースを追跡します。

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

構文の説明

group_tag	設定済みのアカウンティング サーバまたはサーバ グループを指定します。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、アカウンティング サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが、webvpn コンフィギュレーション モードではなく、トンネル グループ一般属性コンフィギュレーション モードで使用できるようになりました。

使用上のガイドライン

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性コンフィギュレーション モードの同等のコマンドに変換されます。

例

トンネル グループ一般属性コンフィギュレーション モードでの次の例では、IPSec LAN-to-LAN トンネル グループ「xyz」に対して「aaa-server123」という名前のアカウンティング サーバ グループを設定します。

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general-attributes
```

```
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)#
```

次に、POP3SSVRS という名前の一連のアカウンティング サーバを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

関連コマンド

コマンド	説明
aaa-server	認証、許可、およびアカウンティング サーバを設定します。

CHAPTER 3

acl-netmask-convert コマンド～ auto-update timeout コマンド

acl-netmask-convert

RADIUS サーバから受信したダウンロード可能な ACL 内のネットマスクをセキュリティ アプライアンスでどのように扱うかを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **acl-netmask-convert** コマンドを使用します。このモードには、**aaa-server host** コマンドを使用してアクセスできます。指定したセキュリティ アプライアンスの動作を削除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

構文の説明

auto-detect	セキュリティ アプライアンスは、使用されているネットマスク表現のタイプを判断しようとします。ワイルドカード ネットマスク表現を検出した場合は、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	セキュリティ アプライアンスは、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
wildcard	セキュリティ アプライアンスは、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ コンフィギュレーション ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバから提供されるダウンロード可能な ACL にワイルドカード形式のネットマスクが含まれている場合は、wildcard または auto-detect キーワードを指定して **acl-netmask-convert** コマンドを使用します。セキュリティ アプライアンスは、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると想定しま

す。ワイルドカード マスクでは、無視するビット位置に 1、照合するビット位置に 0 が配置されます。**acl-netmask-convert** コマンドを使用すると、このような相違が RADIUS サーバ上のダウンロード可能な ACL の設定方法に与える影響を最小限に抑えることができます。

RADIUS サーバの設定方法が不明な場合は、**auto-detect** キーワードが役立ちます。ただし、「穴」があるワイルドカード ネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可し、Cisco VPN 3000 シリーズ コンセントレータでは有効に使用できます。ただし、セキュリティ アプライアンスでは、この表現をワイルドカード ネットマスクとして検出できません。

例

次に、ホスト「192.168.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスクの変換をイネーブルにして、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

action

アクセス ポリシーをセッションに適用するか、またはセッションを終了するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **action** コマンドを使用します。

セッションをリセットしてアクセス ポリシーをセッションに適用するには、このコマンドの **no** 形式を使用します。

action {continue | terminate}

no action {continue | terminate}

構文の説明

continue	アクセス ポリシーをセッションに適用します。
terminate	接続を切断します。

デフォルト

デフォルト値は continue です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

選択したすべての DAP レコードでセッションにアクセス ポリシーを適用するには、**continue** キーワードを使用します。選択した DAP レコードのいずれかで接続を切断するには、**terminate** キーワードを使用します。

例

次に、Finance という DAP ポリシーのセッションを切断する例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# action terminate
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

action-uri

Web サーバの URI を指定して、シングル サインオン認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。

action-uri *string*

no action-uri

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	認証プログラムの URI。複数行に入力できます。各行の最大文字数は 255 です。URI 全体の最大文字数は、2048 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

Uniform Resource Identifier（URI; ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトなストリングです。これらのコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、プログラムなどがあります。URI の最も一般的な形式は、Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式またはサブセットで、URL と呼ばれます。

セキュリティ アプライアンスの WebVPN サーバは、POST 要求を使用して、シングル サインオン認証要求を認証 Web サーバに送信できます。これを行うには、HTTP POST 要求を使用して、認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すようにセキュリティ アプライアンスを設定します。**action-uri** コマンドでは、セキュリティ アプライアンスが POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI を見つけるには、ブラウザで直接 Web サーバのログイン ページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバのアクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時にセキュリティ アプライアンスによって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それよりも少ない文字を各行に入力できます。

（注） ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、www.example.com の URI を指定する例を示します。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
hostname(config)# aaa-server testgrp1 host www.example.com
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

（注） アクション URI にホスト名とプロトコルを含める必要があります。上記の例では、これらは URI の最初にある http://www.example.com に含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

activation-key

セキュリティ アプライアンス のアクティベーション キーを変更し、セキュリティ アプライアンス上で運用されているアクティベーション キーを、セキュリティ アプライアンスのフラッシュ メモリに非表示のファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。セキュリティ アプライアンスで実行されている、指定したアクティベーション キーを無効にするには、このコマンドの **no** 形式を使用します。

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

no activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

構文の説明

activation-key-four-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。
activation-key-five-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	•	•		•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

各要素の間にスペースを 1 つ入れて、4 つの要素で構成される 16 進数文字列として *activation-key-four-tuple* を入力します。または、各要素の間にスペースを 1 つ入れて、5 つの要素で構成される 16 進数文字列として、*activation-key-five-tuple* を入力します。次に例を示します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

例

次に、セキュリティ アプライアンスのアクティベーション キーを変更する例を示します。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

関連コマンド

コマンド	説明
show activation-key	アクティベーション キーを表示します。

activex-relay

WebVPN セッションの ActiveX コントロールをイネーブルまたはディセーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **activex-relay** コマンドを使用します。デフォルトのグループ ポリシーから **activex-relay** コマンドを継承するには、このコマンドの **no** 形式を使用します。

activex-relay {**enable** | **disable**}

no activex-relay

構文の説明

enable	WebVPN セッションの ActiveX をイネーブルにします。
disable	WebVPN セッションの ActiveX をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

activex-relay enable コマンドを使用すると、ユーザは WebVPN ブラウザから ActiveX コントロールを起動できます。これらのアプリケーションでは、WebVPN セッションを使用して ActiveX コントロールをダウンロードおよびアップロードします。ActiveX リレーは、WebVPN セッションが閉じるまで有効です。

例

次のコマンドは、特定のグループ ポリシーに関連付けられている WebVPN セッションの ActiveX コントロールをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

次のコマンドは、特定のユーザ名に関連付けられている WebVPN セッションの ActiveX コントロールをディセーブルにします。

```
hostname(config-username-policy)# webvpn
```

```
hostname(config-username-webvpn)# activex-relay disable
hostname(config-username-webvpn)
```

address-pool（トンネル グループ一般属性モード）

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プール設定は、トンネル グループの **address-pool** コマンドによるローカル プール設定を上書きします。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードで、IPSec リモート アクセス トンネル グループ テスト用にアドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定する例を示します。

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

address-pools（グループ ポリシー属性コンフィギュレーション モード）

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、グループ ポリシー属性コンフィギュレーション モードで **address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールを設定しないことを指定し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用する最大 6 個のアドレス プールのリストを指定します。

デフォルト

デフォルトでは、アドレス プールの属性は継承を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

address-pools none コマンドは、この属性が他のポリシー（DefaultGrpPolicy など）から継承されないようにします。**no address pools none** コマンドは、**address-pools none** コマンドをコンフィギュレーションから削除して、デフォルト値（継承の許可）に戻します。

例

次に、GroupPolicy1 の設定一般コンフィギュレーション モードで、アドレスをリモート クライアントに割り当てるために使用するアドレス プールのリストとして pool_1 および pool_20 を設定する例を示します。

```
hostname(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool_1 pool_20
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN グループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

admin-context

システム コンフィギュレーションの管理コンテキストを設定するには、グローバル コンフィギュレーション モードで **admin-context** コマンドを使用します。システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワーク設定は含まれません。代わりに、システムは、ネットワーク リソースにアクセスする必要がある場合に（セキュリティ アプライアンス ソフトウェアをダウンロードしたり、管理者に対してリモート アクセスを許可する場合など）、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

admin-context *name*

構文の説明

name	名前を最大 32 文字のストリングで設定します。コンテキストをまだ定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。次に、**context** コマンドを使用して最初に追加するコンテキストを、指定した管理コンテキスト名にする必要があります。 この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

デフォルト

マルチ コンテキスト モードの新しいセキュリティ アプライアンスの場合、管理コンテキスト名は「admin」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コンテキスト コンフィギュレーションが内部フラッシュ メモリにある限り、任意のコンテキストを管理コンテキストに設定できます。

現在の管理コンテキストを削除するには、**clear configure context** コマンドを使用してすべてのコンテキストを削除する必要があります。

例

次に、管理コンテキストを「administrator」に設定する例を示します。

```
hostname(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show admin-context	現在の管理コンテキスト名を表示します。

alias

アドレスを手動で変換し、DNS 応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** コマンドを削除するには、このコマンドの **no** 形式を使用します。

alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

no alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

構文の説明

(*interface_name***)**	マッピングされた IP アドレス宛てのトラフィック用の入力インターフェイス（またはマッピングされた IP アドレスからのトラフィック用の出力インターフェイス）の名前を指定します。コマンドにカッコを含めてください。
mapped_ip	実際の IP アドレスの変換先 IP アドレスを指定します。
netmask	（任意）両方の IP アドレスのサブネット マスクを指定します。ホスト マスクの場合は、**255.255.255.255** と入力します。
real_ip	実際の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの機能は、外部 NAT コマンド（**dns** キーワードを指定した **nat** コマンドや **static** コマンド）に置き換えられています。**alias** コマンドの代わりに、外部 NAT コマンドを使用することを推奨します。

宛先アドレスに対してアドレス変換を実行するには、このコマンドを使用します。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用して、トラフィックを 209.165.201.30 などの別のアドレスにリダイレクトします。

（注） **alias** コマンドを他のアドレスの変換ではなく DNS の書き換えに使用する場合は、エイリアス対応インターフェイスで **proxy-arp** をディセーブルにします。セキュリティ アプライアンスが一般的な NAT 処理のために **proxy-arp** でトラフィックを自身に引き寄せないようにするには、**sysopt noproxyarp** コマンドを使用します。

alias コマンドを変更または削除した後は、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルに、**alias** コマンド内の「dnat」アドレスの A（アドレス）レコードが存在している必要があります。

alias コマンドには 2 つの使用方法があります。次にその概略を示します。

- セキュリティ アプライアンスが *mapped_ip* 宛てのパケットを取得した場合は、そのパケットを *real_ip* に送信するように **alias** コマンドを設定できます。
- セキュリティ アプライアンスがセキュリティ アプライアンスに戻された *real_ip* 宛ての DNS パケットを取得した場合は、DNS パケットを変更して、宛先ネットワーク アドレスを *mapped_ip* に変更するように **alias** コマンドを設定できます。

alias コマンドは、自動的にネットワーク上の DNS サーバと通信して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

real_ip IP アドレスと *mapped_ip* IP アドレスにネットワーク アドレスを使用して、ネット エイリアスを指定します。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

static コマンドと **access-list** コマンドで **alias** *mapped_ip* アドレスにアクセスするには、**access-list** コマンドで、許可されるトラフィックの発信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答がセキュリティ アプライアンスによって 192.168.201.29 に変更されます。セキュリティ アプライアンスがグローバル プール IP アドレスとして 209.165.200.225 ～ 209.165.200.254 を使用する場合、パケットは SRC=209.165.201.2 および DST=192.168.201.29 でセキュリティ アプライアンスに送信されます。セキュリティ アプライアンスは、アドレスを外部の SRC=209.165.200.254 と DST=209.165.201.29 に変換します。

例

次に、内部ネットワークに IP アドレス 209.165.201.29 が含まれている例を示します。このアドレスはインターネット上にあり、example.com に属しています。内部クライアントが example.com にアクセスしようとしても、209.165.201.29 はローカルの内部ネットワーク上にあると見なされるため、パケットはセキュリティ アプライアンスに送信されません。この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次に、内部の 10.1.1.11 にある Web サーバと 209.165.201.11 で作成された **static** コマンドの例を示します。ソース ホストは外部にあり、アドレスは 209.165.201.7 です。外部の DNS サーバには、次に示すように www.example.com のレコードがあります。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは 必要です。

次に、**alias** コマンドの使用例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

セキュリティ アプライアンス は、内部クライアント用のネームサーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq
telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。
clear configure alias	すべての **alias** コマンドをコンフィギュレーションから削除します。
show running-config alias	コンフィギュレーション内のデュアル NAT コマンドと重複しているアドレスを表示します。
static	ローカル IP アドレスをグローバル IP アドレスに、またはローカル ポートをグローバル ポートにマッピングすることによって、1 対 1 のアドレス変換ルールを設定します。

allocate-interface

インターフェイスをセキュリティ コンテキストに割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。インターフェイスをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

構文の説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。

map_name	（任意）マッピング名を設定します。
	
	map_name は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているインターフェイスをコンテキスト管理者に知らせない場合があります。
	
	マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。
	
	`int0`
	
	`inta`
	
	`int_0`
	
	サブインターフェイスの場合は、マッピング名の範囲を指定できます。
	
	範囲の詳細については、「使用上のガイドライン」を参照してください。

physical_interface	**gigabitethernet0/1** などのインターフェイス ID を設定します。有効値については、**interface** コマンドを参照してください。インターフェイス タイプとポート番号の間にスペースを含めないでください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（任意）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで物理インターフェイスのプロパティを表示できるようにします。

デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力にインターフェイス ID は表示されません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示設定を変更するには、特定のインターフェイス ID に対してコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、セキュリティ アプライアンスによって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注）　トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、コマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、コマンドは失敗します。

例

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

allocate-ips

IPS 仮想センサーをセキュリティ コンテキストに割り当てるには、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	（任意）コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** *sensor_name* コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
mapped_name	（任意）コンテキスト内で実際のセンサー名の代わりに使用できるセンサー名のエイリアスとして、マッピング名を設定します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM に設定されているセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定した場合は、エラーが表示されますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM にその名前のセンサーが作成されるまで、コンテキストはそのセンサーがダウンしていると見なします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するようにコンテキストを設定するときに、コンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注） 仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。両方のコンテキストで、センサー名を「ips1」と「ips2」にマッピングします。コンテキスト A では sensor1 をデフォルト センサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show ips	AIP SSM に設定されている仮想センサーを表示します。

apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn コンフィギュレーション モードで **apcf** コマンドを使用します。特定の APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を使用します。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL/filename.ext

no apcf [URL/filename.ext]

構文の説明

filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは、常に XML 形式です。拡張子は、.xml、.txt、.doc などです。
URL	セキュリティ アプライアンスでロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバ、ポート、およびパスを含めることができます。ファイル名のみを指定した場合、デフォルトの URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

apcf コマンドを使用すると、セキュリティ アプライアンスは、非標準の Web アプリケーションと Web リソースを WebVPN 接続で正しくレンダリングされるように処理できます。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。

セキュリティ アプライアンスで複数の APCF プロファイルを使用できます。その場合、セキュリティ アプライアンスは、それらのプロファイルを古いものから新しいものの順に 1 つずつ適用します。

apcf コマンドは、Cisco TAC のサポートがある場合にのみ使用することを推奨します。

例

次に、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

次に、myserver という名前の https サーバ（ポート 1440）のパス /apcf にある apcf2.xml という名前の APCF をイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。
rewrite	トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。
show running config webvpn apcf	APCF 設定を表示します。

appl-acl

セッションに適用する設定済みの Web タイプ ACL を指定するには、DAP webvpn コンフィギュレーション モードで **appl-acl** コマンドを使用します。属性をコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。すべての Web タイプ ACL を削除するには、このコマンドの **no** 形式を引数なしで使用します。

appl-acl *identifier*

no appl-acl [*identifier***]**

構文の説明

identifier	設定済みの Web タイプ ACL の名前（最大 240 文字）。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

Web タイプ ACL を設定するには、グローバル コンフィギュレーション モードで **access-list_webtype** コマンドを使用します。

appl-acl コマンドを複数回使用して、複数の Web タイプ ACL を DAP ポリシーに適用できます。

例

次に、newacl という名前の設定済みの Web タイプ ACL をダイナミック アクセス ポリシーに適用する例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# appl-acl newacl
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
access-list_webtype	Web タイプ ACL を作成します。

application-access

認証された WebVPN ユーザに表示される WebVPN ホームページの [Application Access] フィールド、およびユーザがアプリケーションを選択したときに表示される [Application Access] ウィンドウをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **application-access** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

構文の説明

message	[Application Access] フィールドのタイトルの下に表示されるメッセージを変更します。
style	[Application Access] フィールドのスタイルを変更します。
text	[Application Access] フィールドのテキストを変更します。
title	[Application Access] フィールドのタイトルを変更します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。
window	[Application Access] ウィンドウを変更します。

デフォルト

[Application Access] フィールドのデフォルトのタイトル テキストは「Application Access」です。

[Application Access] フィールドのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

[Application Access] フィールドのデフォルトのメッセージ テキストは「Start Application Client」です。

[Application Access] フィールドのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

[Application Access] ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access.Please wait for the table to be displayed before starting applications.」

[Application Access] ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

次に、WebVPN ページに対する変更で最もよく行われるページ配色の変更に役立つヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Application Access] フィールドの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	[Application Access] ウィンドウのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN の [Application Access] ウィンドウに表示されるアプリケーション詳細を非表示にするには、カスタマイゼーション コンフィギュレーション モードで **application-access hide-details** コマンドを使用します。このモードには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access hide-details {**enable | disable**}

no application-access [**hide-details** {**enable | disable**}]

構文の説明

disable	[Application Access] ウィンドウにアプリケーション詳細を表示します。
enable	[Application Access] ウィンドウのアプリケーション詳細を非表示にします。

デフォルト

デフォルトではディセーブルになっています。[Application Access] ウィンドウにアプリケーション詳細が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、アプリケーション詳細の表示をディセーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] フィールドをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。

area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

構文の説明

area_id	作成するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

作成したエリアには、パラメータが設定されていません。関連する area コマンドを使用してエリア パラメータを設定します。

例

次に、エリア ID が 1 の OSPF エリアを作成する例を示します。

```
hostname(config-router)# area 1
hostname(config-router)#
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。

エリア認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

構文の説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
message-digest	（任意）*area_id* で指定したエリアに対する Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリア認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定した OSPF エリアが存在しない場合は、このコマンドを入力すると作成されます。**message-digest** キーワードを指定せずに **area authentication** コマンドを入力した場合は、簡易パスワード認証がイネーブルになります。**message-digest** キーワードを指定すると、MD5 認証がイネーブルになります。

例

次に、エリア 1 に対して MD5 認証をイネーブルにする例を示します。

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area default-cost

スタブまたは NSSA に送信されるデフォルト集約ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost**

構文の説明

area_id	デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
cost	スタブまたは NSSA に使用されるデフォルト集約ルートのコストを指定します。有効な値の範囲は、0 ～ 65535 です。

デフォルト

cost のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

例

次に、スタブまたは NSSA に送信される集約ルートのデフォルト コストを指定する例を示します。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

構文の説明

area_id	フィルタリングを設定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
in	指定したエリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定したエリアから発信されるアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワークに ASBR が設定されている場合、ASBR はプライベート ネットワークを記述するタイプ 5 LSA を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッディングされます。

例

次に、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングする例を示します。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。NSSA 指定をエリアから削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

構文の説明

area_id	NSSA として指定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR または NSSA ASBR でのみ有効です。
metric *metric_value*	（任意）OSPF デフォルト メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。
metric-type {**1** | **2**}	（任意）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • **1**：タイプ 1 • **2**：タイプ 2 デフォルト値は 2 です。
no-redistribution	（任意）ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA エリアでなく通常のエリアにのみ取り込む場合に使用します。
no-summary	（任意）エリアを Not-So-Stubby Area（NSSA）とし、集約ルートが挿入されないようにします。

デフォルト

デフォルトの設定は次のとおりです。

- NSSA エリアは未定義です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

エリアに 1 つのオプションを設定し、後で別のオプションを指定した場合、両方のオプションが設定されます。たとえば、次の 2 のコマンドを別々に入力した場合、コンフィギュレーションには、両方のオプションを指定した 1 つのコマンドが設定されます。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

例

次に、2 つのオプションを別々に設定すると、1 つのコマンドがコンフィギュレーションに設定される例を示します。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area range

エリア境界でルートを統合および集約するには、ルータ コンフィギュレーション モードで **area range** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

構文の説明

address	サブネット範囲の IP アドレス。
advertise	（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。
area_id	範囲を設定するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。

デフォルト

アドレス範囲ステータスは advertise に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、ABR でのみ使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は*ルート集約*と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。したがって、OSPF は、多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* **not-advertise** コマンドは、**not-advertise** オプション キーワードのみを削除します。

例

次に、ネットワーク 10.0.0.0 上のすべてのサブネットおよびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つの集約ルートを、ABR によって他のエリアにアドバタイズするように指定する例を示します。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリア機能を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* [**no-summary**]

no area *area_id* [**no-summary**]

構文の説明

area_id	スタブ エリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアは定義されません。
- サマリー リンク アドバタイズメントはスタブ エリアに送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、スタブまたは NSSA に接続された ABR でのみ使用されます。

スタブ エリア ルータ コンフィギュレーション コマンドには、**area stub** および **area default-cost** という 2 つのコマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続された ABR でのみ **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成される集約デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次に、指定したエリアをスタブ エリアとして設定する例を示します。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト集約ルートのコストを指定します。
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

構文の説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
authentication	（任意）認証タイプを指定します。
authentication-key *key*	（任意）ネイバー ルーティング デバイスで使用する OSPF 認証パスワードを指定します。
dead-interval *seconds*	（任意）hello パケットを受信しない場合に、ネイバー ルーティング デバイスがダウンしたことを宣言するまでの間隔を指定します。有効な値は、1 ～ 65535 秒です。
hello-interval *seconds*	（任意）インターフェイスで送信される hello パケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。
md5 *key*	（任意）最大 16 バイトの英数字のキーを指定します。
message-digest	（任意）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（任意）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は、1 ～ 255 です。
null	（任意）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されている場合、上書きされます。
retransmit-interval *seconds*	（任意）インターフェイスに属している隣接ルータの LSA 再送信の間隔を指定します。有効な値は、1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は、各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（任意）OSPF がトポロジ変更を受信してから、Shortest Path First（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒で指定します。デフォルトは 5 秒です。

デフォルト

デフォルトの設定は次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- **hello-interval** *seconds*：10 秒。
- **retransmit-interval** *seconds*：5 秒。

- **transmit-delay** *seconds*：1 秒。
- **dead-interval** *seconds*：40 秒。
- **authentication-key** *key*：キーは事前に定義されていません。
- **message-digest-key** *key_id* **md5** *key*：キーは事前に定義されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、**area** *area_id* **authentication** コマンドでバックボーンに対して認証がイネーブルにされている場合にのみ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらか一方を指定するか、または両方とも指定しないでください。**authentication-key** *key* または **message-digest-key** *key_id* **md5** *key* の後に指定したキーワードと引数は、すべて無視されます。したがって、オプションの引数は、これらのキーワードと引数の組み合わせの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスでは、エリアに指定されている認証タイプが使用されます。エリアに認証タイプが指定されていない場合、エリアのデフォルトはヌル認証です。

（注） 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンクからオプションを削除するには、削除するオプションを指定して、このコマンドの **no** 形式を使用します。仮想リンクを削除するには、**no area** *area_id* **virtual-link** コマンドを使用します。

例

次に、MD5 認証の仮想リンクを確立する例を示します。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

arp

スタティック ARP エントリを ARP テーブルに追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。スタティック ARP エントリは、MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトせず、ネットワーク問題の解決に役立つ場合があります。トランスペアレント ファイアウォール モードでは、ARP インスペクションでスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

構文の説明

alias	（任意）このマッピングに対してプロキシ ARP をイネーブルにします。セキュリティ アプライアンスは、指定された IP アドレスに対する ARP 要求を受信すると、セキュリティ アプライアンスの MAC アドレスで応答します。その IP アドレスを持つホスト宛てのトラフィックをセキュリティ アプライアンスが受信すると、セキュリティ アプライアンスは、トラフィックをこのコマンドで指定されたホスト MAC アドレスに転送します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。 トランスペアレント ファイアウォール モードでは、このキーワードは無視され、セキュリティ アプライアンスでプロキシ ARP は実行されません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求

を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリがセキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイス上の 10.1.1.1 と MAC アドレス 0009.7cbe.2100 のスタティック ARP エントリを作成する例を示します。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp timeout

セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

arp timeout *seconds*

no arp timeout *seconds*

構文の説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

デフォルト

デフォルト値は 14,400 秒（4 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ARP タイムアウトを 5,000 秒に変更する例を示します。

```
hostname(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp-inspection

トランスペアレント ファイアウォール モードでの ARP インスペクションをイネーブルにするには、グローバル コンフィギュレーション モードで **arp-inspection** コマンドを使用します。ARP インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。ARP インスペクションでは、すべての ARP パケットをスタティック ARP エントリと照合し（**arp** コマンドを参照）、一致しないパケットをブロックします。この機能により、ARP スプーフィングが防止されます。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

構文の説明

enable	ARP インスペクションをイネーブルにします。
flood	（デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットをすべてのインターフェイス（発信元インターフェイスを除く）にフラッディングすることを指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。 **（注）** 管理専用のインターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。
interface_name	ARP インスペクションをイネーブルにするインターフェイス。
no-flood	（任意）スタティック ARP エントリと正確には一致しないパケットをドロップすることを指定します。

デフォルト

デフォルトでは、ARP インスペクションはすべてのインターフェイスでディセーブルになっています。すべての ARP パケットはセキュリティ アプライアンスを通過できます。ARP インスペクションをイネーブルにすると、一致しない ARP パケットはデフォルトでフラッディングされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ARP インスペクションをイネーブルにする前に、**arp** コマンドを使用してスタティック ARP エントリを設定します。

ARP インスペクションをイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにセキュリティ アプライアンスを設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリがセキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイスにおける ARP インスペクションをイネーブルにし、スタティック ARP エントリに一致しない ARP パケットをドロップするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP インスペクション コンフィギュレーションをクリアします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

構文の説明

session	終了するアクティブな ASDM セッションのセッション ID。**show asdm sessions** コマンドを使用して、すべてのアクティブな ASDM セッションのセッション ID を表示できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm disconnect** コマンドが **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのアクティブな ASDM セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM セッションにはセッション ID 1 が割り当てられ、その後の新しいセッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect** コマンドの入力の前後に、**show asdm sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions
```

```
1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

asdm disconnect log_session *session*

構文の説明

session	終了するアクティブな ASDM ロギング セッションのセッション ID。**show asdm log_sessions** コマンドを使用して、すべてのアクティブな ASDM セッションのセッション ID を表示できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから Syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶ場合があります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギング セッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

ASDM ロギング セッションを終了しても、残りのアクティブな ASDM ロギング セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM ロギング セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM ロギング セッションにはセッション ID 1 が割り当てられ、その後の新しいロギング セッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect log_sessions** コマンドの入力の前後に、**show asdm log_sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm history enable

ASDM 履歴トラッキングをイネーブルにするには、グローバル コンフィギュレーション モードで **asdm history enable** コマンドを使用します。ASDM 履歴トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

asdm history enable

no asdm history enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pdm history enable** コマンドが **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって取得された情報は、ASDM 履歴バッファに保存されます。この情報は、**show asdm history** コマンドを使用して表示できます。履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次に、ASDM 履歴トラッキングをイネーブルにする例を示します。

```
hostname(config)# asdm history enable
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

フラッシュ メモリ内の ASDM ソフトウェア イメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの場所を削除するには、このコマンドの **no** 形式を使用します。

asdm image *url*

no asdm image [*url*]

構文の説明

url	フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL 構文を参照してください。 • **disk0:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。 • **flash:**/[*path*/]*filename* この URL は内部フラッシュ メモリを示します。

デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。セキュリティ アプライアンスはイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フラッシュ メモリに複数の ASDM ソフトウェア イメージを保存できます。アクティブな ASDM セッションがある状態で **asdm image** コマンドを入力して新しい ASDM ソフトウェア イメージを指定した場合、アクティブな ASDM セッションは中断されず、そのセッションを開始した ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用

します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、セキュリティ アプライアンスから引き続き ASDM にアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。セキュリティ アプライアンスはイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。**write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しない場合、リブートのたびにセキュリティ アプライアンスは ASDM イメージを検索し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update を使用する場合は、起動時にこのコマンドが自動的に追加されるため、セキュリティ アプライアンス上のコンフィギュレーションは Auto Update Server 上のコンフィギュレーションと一致しなくなります。このような不一致が発生すると、セキュリティ アプライアンスはコンフィギュレーションを Auto Update Server からダウンロードします。不要な Auto Update アクティビティを回避するには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存します。

例

次に、ASDM イメージを asdm.bin に設定する例を示します。

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。
boot	ソフトウェア イメージとスタートアップ コンフィギュレーション ファイルを設定します。

asdm location

注意　このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

構文の説明

ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
netmask	*ip_addr* のサブネット マスク。
if_name	ASDM にアクセスするときに通過するインターフェイスの名前。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスとプレフィックス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm location** コマンドが **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*

no asr-group *group_id*

構文の説明

group_id	非対称ルーティング グループ ID。有効な値は、1 ～ 32 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	—	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

Active/Active フェールオーバーがイネーブルの場合、ロード バランシングにより、発信接続のリターン トラフィックがピア ユニット上のアクティブなコンテキストを介してルーティングされることがあります。このピア ユニットでは、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドを使用すると、着信インターフェイスのフローが見つからない場合に、着信パケットが同じ asr-group のインターフェイスで再分類されます。再分類により別のインターフェイスのフローが見つかり、関連付けられているコンテキストがスタンバイ状態の場合、パケットは処理のためにアクティブなユニットに転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーをイネーブルにする必要があります。

ASR 統計情報は、**show interface detail** コマンドを使用して表示できます。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれます。

例

次に、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てる例を示します。

コンテキスト ctx1 のコンフィギュレーション：

```
hostname/ctx1(config)# interface Ethernet2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション：

```
hostname/ctx2(config)# interface Ethernet3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイス統計情報を表示します。

assertion-consumer-url

セキュリティ デバイスがアサーション コンシューマ サービスに接続するためにアクセスする URL を指定するには、webvpn コンフィギュレーション モードで、特定の SAML-type SSO サーバに対して **assertion-consumer-url** コマンドを使用します。

この URL をアサーションから削除するには、このコマンドの **no** 形式を使用します。

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

構文の説明

url	SAML-type SSO サーバで使用するアサーション コンシューマ サービスの URL を指定します。URL は http:// または https: で始まり、255 文字未満の英数字である必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

URL が HTTPS で始まる場合は、アサーション コンシューマ サービスの SSL 証明書のルート証明書をインストールする必要があります。

次に、SAML-type の SSO サーバのアサーション コンシューマ URL を指定する例を示します。

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
hostname(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
issuer	SAML-type の SSO サーバのセキュリティ デバイス名を指定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	WebVPN シングル サインオン サーバを作成します。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

attribute

セキュリティ アプライアンスが DAP 属性データベースに書き込む属性値ペアを指定するには、DAP テスト属性モードで **attribute** コマンドを使用します。複数の属性値ペアを入力するには、このコマンドを複数回使用します。

attribute *name value*

構文の説明

name	既知の属性名、または「label」タグを組み込む属性を指定します。label タグは、DAP レコード内のファイル、レジストリ、プロセス、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのエンドポイント属性に対して設定するエンドポイント ID に対応します。
value	AAA 属性に割り当てられた値。

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP 属性コンフィギュレーション モード	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

例

次の例では、認証されたユーザが SAP グループのメンバーで、エンドポイント システムにアンチウイルス ソフトウェアがインストールされている場合に、セキュリティ アプライアンスが 2 つの DAP レコードを選択することを前提としています。アンチウイルス ソフトウェアのエンドポイント ルールのエンドポイント ID は *nav* です。

DAP レコードには、次のポリシー属性があります。

DAP レコード 1	DAP レコード 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
	url-entry = enable

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
hostname(config-dap-test-attr)# attribute endpoint.av.nav.exists true
hostname(config-dap-test-attr)# exit

hostname # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

hostname #
```

関連コマンド

コマンド	説明
display	現在の属性リストを表示します。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセス ポリシーをコンソールに表示します。

auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

auth-cookie-name

構文の説明

name	認証クッキーの名前。名前の最大の長さは 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。認証が成功すると、認証 Web サーバは、認証クッキーをクライアント ブラウザに戻します。クライアント ブラウザは、その認証クッキーを提示して、SSO ドメイン内の他の Web サーバの認証を受けます。**auth-cookie-name** コマンドは、セキュリティ アプライアンスによって SSO に使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: <cookie name>=<cookie value> [;<cookie attributes>] です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5d
c/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Pa
th=/
```

例

次に、example.com という名前の Web サーバから受信した認証クッキーに認証クッキー名 SMSESSION を指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	ユーザ名パラメータを SSO 認証に使用される HTTP POST 要求の一部として送信する必要があることを指定します。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

構文の説明

interface-name	接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。 • **inside**　GigabitEthernet0/1 インターフェイスの名前 • **outside**　GigabitEthernet0/0 インターフェイスの名前

デフォルト

- **authentication-certificate** コマンドを省略すると、クライアント証明書認証はディセーブルになります。
- interface-name を **authentication-certificate** コマンドで指定しない場合、デフォルトの interface-name は **inside** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでにイネーブルになっている必要があります。インターフェイスを設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、管理接続のクライアント証明書認証を **http authentication-certificate** コマンドを使って指定することは、WebVPN をサポートしないプラットフォームも含めてすべてのプラットフォームで可能です。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
セキュリティ アプライアンスに組み込まれているローカル CA がイネーブルでない場合。	セキュリティ アプライアンスは SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	セキュリティ アプライアンスは証明書を取得するために、クライアントをローカル CA の証明書登録ページにリダイレクトします。
ローカル CA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカル CA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザ接続の証明書認証を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication（トンネル グループ **webvpn** コンフィギュレーション モード）	トンネル グループのメンバーは認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	認証にセキュリティ アプライアンスへの ASDM 管理接続用の証明書を使用することを指定します。
interface	接続の確立に使用するインターフェイスを設定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl trust-point	SSL 証明書トラストポイントを設定します。

authentication-exclude

エンド ユーザがクライアントレス SSL VPN にログインせずに設定済みリンクを参照できるようにするには、webvpn モードで **authentication-exclude** コマンドを使用します。複数のサイトへのアクセスを許可するには、このコマンドを複数回使用します。

authentication-exclude *url-fnmatch*

構文の説明

url-fnmatch	クライアントレス SSL VPN へのログインの要件を免除するリンクを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

この機能は、一部の内部リソースを SSL VPN 経由で一般利用できるようにする場合に便利です。

リンクに関する情報を、SSL VPN マングリングした形式でエンド ユーザに配布する必要があります。たとえば、SSL VPN を使用してこれらのリソースを参照し、配布するリンクに関する情報に結果の URL をコピーします。

例

次に、2 つのサイトに対して認証要件を免除する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-exclude http://www.site.com/public/*
hostname(config-webvpn)#authentication-exclude *announcement.html
hostname(config-webvpn)# hostname #
```

authentication

WebVPN と電子メール プロキシの認証方式を設定するには、各モードで **authentication** コマンドを使用します。デフォルトの方式に戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、ユーザを認証してユーザ ID を確認します。

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback**]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

構文の説明

aaa	セキュリティ アプライアンスが設定済みの AAA サーバと照合するユーザ名およびパスワードを指定します。
certificate	SSL ネゴシエーション時の証明書を指定します。
mailhost	リモート メール サーバを介して認証します。SMTPS の場合にのみ使用します。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
piggyback	HTTPS WebVPN セッションがすでに存在している必要があります。ピギーバック認証は、電子メール プロキシでのみ使用できます。

デフォルト

次の表に、WebVPN および電子メール プロキシのデフォルトの認証方式を示します。

プロトコル	デフォルトの認証方式
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA
WebVPN	AAA

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
webvpn コンフィギュレーション	•		•		

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、WebVPN 用のトンネル グループ webvpn 属性コンフィギュレーション モードに置き換えられました。
8.0(2)	このコマンドは、証明書認証要件の変更を反映するように変更されました。

使用上のガイドライン

少なくとも 1 つの認証方式が必要です。たとえば、WebVPN の場合、AAA 認証と証明書認証のいずれか一方または両方を指定できます。これらは、どちらを先に指定してもかまいません。

WebVPN 証明書認証では、それぞれのインターフェイスに対して HTTPS ユーザ証明書を要求する必要があります。つまり、この選択が機能するには、証明書認証を指定する前に、**authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。その場合、ユーザは証明書およびユーザ名とパスワードを指定する必要があります。電子メール プロキシ認証の場合、複数の認証方式を要求できます。このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例

次に、WebVPN ユーザに認証のための証明書を要求する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

関連コマンド

コマンド	説明
authentication-certificate	接続を確立する WebVPN クライアントからの証明書を要求します。
show running-config	現在のトンネル グループ コンフィギュレーションを表示します。
clear configure aaa	設定済みの AAA の値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

authentication eap-proxy

L2TP over IPSec 接続に対して EAP をイネーブルにし、セキュリティ アプライアンスが PPP 認証プロセスを外部の RADIUS 認証サーバにプロキシできるようにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication eap-proxy

no authentication eap-proxy

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、EAP は認証プロトコルとして許可されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、pppremotegrp という名前のトンネル グループの PPP 接続に対して EAP を許可する例を示します。

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

authentication key eigrp

EIGRP パケットの認証をイネーブルにし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **authentication key eigrp** コマンドを使用します。EIGRP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

構文の説明

as-number	認証する EIGRP プロセスの自律システム番号。これは、EIGRP ルーティング プロセスに設定されている値と同じにする必要があります。
key	EIGRP 更新を認証するキー。このキーには、最大 16 文字を含めることができます。
key-id *key-id*	キー ID 値。有効な値の範囲は 1 ～ 255 です。

デフォルト

EIGRP 認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# authentication mode eigrp md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication mode eigrp	EIGRP 認証に使用する認証のタイプを指定します。

authentication mode eigrp

EIGRP 認証に使用する認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **authentication mode eigrp** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

構文の説明

as-num	EIGRP ルーティング プロセスの自律システム番号です。
md5	EIGRP メッセージ認証に MD5 を使用します。

デフォルト

デフォルトでは、認証は提供されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# authentication mode eigrp 100 md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication key eigrp	EIGRP パケットの認証をイネーブルにし、認証キーを指定します。

authentication ms-chap-v1

L2TP over IPSec 接続で PPP の Microsoft CHAP Version 1 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

Microsoft CHAP Version 1 をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication ms-chap-v2

no authentication ms-chap-v2

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication ms-chap-v2

L2TP over IPSec 接続に対して PPP の Microsoft CHAP Version 2 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

Microsoft CHAP バージョン 2 をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication ms-chap-v1

no authentication ms-chap-v1

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication pap

L2TP over IPSec 接続に対して PPP の PAP 認証を許可するには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication pap** コマンドを使用します。このプロトコルは、認証時にクリアテキストのユーザ名とパスワードを渡すため、安全ではありません。

コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication pap

no authentication pap

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、PAP は認証プロトコルとして許可されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、L2TP/IPSec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、ppremotegrp という名前のトンネル グループの PPP 接続に対して PAP を許可する例を示します。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。

コマンド	説明
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

構文の説明

interface-name	接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。 • **inside**　GigabitEthernet0/1 インターフェイスの名前 • **outside**　GigabitEthernet0/0 インターフェイスの名前

デフォルト

- **authentication-certificate** コマンドを省略すると、クライアント証明書認証はディセーブルになります。
- interface-name を **authentication-certificate** コマンドで指定しない場合、デフォルトの interface-name は **inside** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでにイネーブルになっている必要があります。インターフェイスを設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、**管理**接続のクライアント証明書認証を **http authentication-certificate** コマンドを使って指定することは、WebVPN をサポートしないプラットフォームも含めてすべてのプラットフォームで可能です。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
セキュリティ アプライアンスに組み込まれているローカル CA がイネーブルでない場合。	セキュリティ アプライアンスは SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	セキュリティ アプライアンスは証明書を取得するために、クライアントをローカル CA の証明書登録ページにリダイレクトします。
ローカル CA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカル CA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザ接続の証明書認証を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication（トンネル グループ **webvpn** コンフィギュレーション モード）	トンネル グループのメンバーは認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	認証にセキュリティ アプライアンスへの ASDM 管理接続用の証明書を使用することを指定します。
interface	接続の確立に使用するインターフェイスを設定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl trust-point	SSL 証明書トラストポイントを設定します。

authentication-port

特定のホストの RADIUS 認証に使用するポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **authentication-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドでは、認証機能を割り当てるリモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

authentication-port *port*

no authentication-port

構文の説明

port	RADIUS 認証用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートが指定されていない場合、RADIUS 認証のデフォルト ポート番号（1645）が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。

使用上のガイドライン

RADIUS 認証サーバで 1645 以外のポートが使用されている場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートをセキュリティ アプライアンスに設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

authentication-server-group（imap4s、pop3s、smtps）

電子メール プロキシに使用する認証サーバのセットを指定するには、各モードで **authentication-server-group** コマンドを使用します。認証サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、ユーザを認証してユーザ ID を確認します。

authentication-server-group *group_tag*

no authentication-server-group

構文の説明

group_tag	事前に設定済みの認証サーバまたはサーバ グループを指定します。認証サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認証サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

AAA 認証を設定する場合は、この属性も設定する必要があります。設定しないと、認証は常に失敗します。

例

次に、「IMAP4SSVRS」という名前の認証サーバのセットを使用するように IMAP4S 電子メール プロキシを設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。

authentication-server-group（トンネル グループ一般属性）

トンネル グループでユーザ認証に使用する AAA サーバ グループを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **authentication-server-group** コマンドを使用します。この属性をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

構文の説明

interface_name	（任意）IPSec トンネルが終端するインターフェイスを指定します。
LOCAL	（任意）通信障害によりサーバ グループにあるすべてのサーバが非アクティブになった場合に、ローカル ユーザ データベースに対する認証を要求します。サーバ グループ名が **LOCAL** または **NONE** の場合、ここでは **LOCAL** キーワードを使用しないでください。
server_group	事前に設定済みの認証サーバまたはサーバ グループを指定します。

デフォルト

このコマンドのサーバ グループのデフォルト設定は **LOCAL** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
8.0(2)	このコマンドは、インターフェイス単位で IPSec 接続の認証を行えるように拡張されました。

使用上のガイドライン

この属性は、すべてのトンネル グループ タイプに適用できます。

認証サーバを設定するには **aaa-server** コマンドを使用し、設定済みの AAA サーバ グループにサーバを追加するには **aaa-server-host** コマンドを使用します。

例

次に、設定一般コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループに aaa-server456 という名前の認証サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
aaa-server host	設定済みの AAA サーバ グループにサーバを追加し、ホスト固有の AAA サーバ パラメータを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

authorization-dn-attributes

（注）　リリース 8.0(4) 以降このコマンドは廃止されました。このコマンドの代わりに **username-from-certificate** コマンドを使用します。

認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定するには、各コンフィギュレーション モードで **authorization-dn-attributes** コマンドを使用します。属性をコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no authorization-dn-attributes

構文の説明

primary-attr	証明書から認可クエリー用の名前を生成するときに使用する属性を指定します。
secondary-attr	（任意）デジタル証明書から認可クエリー用の名前を生成するときにプライマリ属性と共に使用する追加の属性を指定します。
use-entire-name	セキュリティ アプライアンスでは、完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。

デフォルト

プライマリ属性のデフォルト値は CN（一般名）です。

セカンダリ属性のデフォルト値は OU（組織の部門）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
7.2(1)	imap4s、pop3、および smtps コンフィギュレーション モードが追加されました。

使用上のガイドライン　プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
CN	Common Name（一般名）：個人、システムなどの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
O	Organization（組織）：会社、団体、機関、連合などの名前。
L	Locality（地名）：組織が置かれている市または町。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
EA	電子メール アドレス
T	肩書
N	名前
GN	名
SN	姓
I	イニシャル
GENQ	Generational Qualifier（世代修飾子）
DNQ	Domain Name Qualifier（ドメイン名修飾子）
UID	User Identifier（ユーザ識別子）
UPN	ユーザ プリンシパル名
SER	Serial Number（シリアル番号）
use-entire-name	DN 名全体を使用

例　次の例では、グローバル コンフィギュレーション モードで、remotegrp という IPSec リモート アクセス トンネル グループを作成し、デジタル証明書から認可クエリー用の名前を生成するために CN（Common Name; 一般名）をプライマリ属性として使用することを指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-required

接続前にユーザが正常に認可されることを求めるには、各モードで **authorization-required** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

authorization-required

no authorization-required

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

authorization-required は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
7.2(1)	webvpn コンフィギュレーション モードが imap4s、pop3s、および smtps コンフィギュレーション モードに置き換えられました。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを介して接続するユーザに完全な DN に基づく認可を要求する例を示します。最初のコマンドでは、remotegrp という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPSec リモート アクセス）と設定しています。2 番めのコマンドで、指定したトンネル グループのトンネル グループ一般属性コンフィギュレーション モードを開始し、最後のコマンドで、指定したトンネル グループに認可が必要であることを指定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
authorization-dn-attributes	認可用のユーザ名として使用するプライマリおよびセカンダリ サブジェクト DN フィールドを指定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-server-group

WebVPN および電子メール プロキシに使用する認可サーバのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、認可を使用して、ユーザに許可されているネットワーク リソースへのアクセス レベルを確認します。

authorization-server-group *group_tag*

no authorization-server-group

構文の説明

group_tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認可サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、「POP3Spermit」という名前の許可サーバのセットを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
hostname(config)# pop3s
```

```
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

次に、設定一般コンフィギュレーション モードで、「remotegrp」という名前の IPSec リモート アクセス トンネル グループに「aaa-server78」という名前の許可サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

auth-prompt

セキュリティ アプライアンスを介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキストを削除するには、このコマンドの **no** 形式を使用します。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

構文の説明

accept	Telnet 経由のユーザ認証を受け入れる場合、プロンプトとして *string* を表示します。
prompt	このキーワードの後に AAA チャレンジ プロンプトのストリングを入力します。
reject	Telnet 経由のユーザ認証を拒否する場合、プロンプトとして *string* を表示します。
string	235 文字または 30 単語（どちらか最初に達した方）までの英数字で構成されるストリング。特殊文字、スペース、および句読点を使用できます。疑問符を入力するか、または Enter キーを押すと、ストリングが終了します （疑問符はストリングに含まれます）。

デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示されます。
- HTTP ユーザには `HTTP Authentication` が表示されます。
- Telnet ユーザにはチャレンジ テキストが表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	セマンティックに小さな変更が加えられました。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要な場合に、セキュリティ アプライアンス経由の HTTP、FTP、および Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

Telnet からのユーザ認証が行われる場合、**accept** オプションと **reject** オプションを使用して、認証試行が AAA サーバによって受け入れられたか拒否されたかを示す各ステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、セキュリティ アプライアンスは **auth-prompt accept** テキスト（指定されている場合）をユーザに表示します。ユーザが認証されない場合は、**reject** テキスト（指定されている場合）を表示します。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。**accept** テキストと **reject** テキストは表示されません。

（注） Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Telnet および FTP では、認証プロンプトに最大 235 文字表示されます。

例

次に、認証プロンプトを「Please enter your username and password」というストリングに設定する例を示します。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

このストリングがコンフィギュレーションに追加されると、ユーザには次のように表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、セキュリティ アプライアンスが認証試行を受け入れたときに表示されるメッセージと拒否したときに表示されるメッセージを別々に指定できます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次に、認証に成功した場合の認証プロンプトを「You're OK.」というストリングに設定する例を示します。

```
hostname(config)# auth-prompt accept You're OK.
```

認証に成功すると、ユーザには次のメッセージが表示されます。

```
You're OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプト チャレンジ テキスト（ある場合）を削除し、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-signon

クライアントレス SSL VPN 接続用のユーザ ログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。認証方式は、NTLM（NTLMv1 と NTLMv2 を含む）と HTTP 基本認証のいずれか一方、または両方にすることができます。特定のサーバへの自動サインオンをディセーブルにするには、元の **ip**、**uri**、および **auth-type** 引数を指定して、このコマンドの **no** 形式を使用します。すべてのサーバへの自動サインオンをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}]

構文の説明

all	NTLM と HTTP 基本認証の両方の方式を指定します。
allow	特定のサーバに対する認証をイネーブルにします。
auth-type	認証方式の選択をイネーブルにします。
basic	HTTP 基本認証方式を指定します。
ftp	FTP および CIFS 認証タイプを指定します。
ip	IP アドレスとマスクで認証先のサーバを特定することを指定します。
ip-address	*ip-mask* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ip-mask	*ip-address* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ntlm	NTLMv1 認証方式を指定します。
resource-mask	認証先のサーバの URI マスクを指定します。
uri	URI マスクで認証先のサーバを特定することを指定します。

デフォルト

デフォルトでは、この機能はすべてのサーバでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション（グローバル）	•	—	•	—	—
webvpn グループ ポリシー コンフィギュレーション	•	—	•	—	—
WebVPN ユーザ名コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(1)	NTLMv2 のサポートが追加されました。**ntlm** キーワードには、NTLMv1 と NTLMv2 の両方が含まれます。

使用上のガイドライン

auto-signon コマンドは、クライアントレス SSL VPN ユーザのためのシングル サインオン方式です。この方式では、ログイン クレデンシャル（ユーザ名とパスワード）を NTLM 認証と HTTP Basic 認証のいずれか一方または両方を使用する認証用の内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

auto-signon 機能は、webvpn コンフィギュレーション グループ ポリシー モード、webvpn コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作が適用されます。つまり、グループよりもユーザ名が優先され、グローバルよりもグループが優先されます。モードは、認証の目的範囲に基づいて選択します。

モード	スコープ
webvpn コンフィギュレーション	すべての WebVPN ユーザ（グローバル）
webvpn グループ コンフィギュレーション	グループ ポリシーで定義される WebVPN ユーザのサブセット
WebVPN ユーザ名コンフィギュレーション	個々の WebVPN ユーザ

例

次に、NTLM 認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

次に、HTTP 基本認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

次に、HTTP 基本認証または NTLM 認証を使用して、クライアントレス ユーザの ExamplePolicy グループに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに自動サインオンを設定する例を示します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

次に、HTTP 基本認証を使用して、Anyuser という名前のユーザに自動サインオンを設定するコマンドの例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

関連コマンド

コマンド	説明
show running-config webvpn auto-signon	実行コンフィギュレーションの自動サインオンの割り当てを表示します。

auto-summary

ネットワークレベル ルートへのサブネット ルートの自動集約をイネーブルにするには、ルータ コンフィギュレーション モードで **auto-summary** コマンドを使用します。ルート集約をディセーブルにするには、このコマンドの **no** 形式を使用します。

auto-summary

no auto-summary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ルート集約は、RIP バージョン 1、RIP バージョン 2、および EIGRP でイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	EIGRP のサポートが追加されました。

使用上のガイドライン

ルート集約により、ルーティング テーブルにおけるルーティング情報の量が少なくなります。

RIP バージョン 1 では、常に自動集約が使用されます。RIP バージョン 1 に対して自動集約をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

EIGRP 集約ルートには、アドミニストレーティブ ディスタンス値 5 が割り当てられます。この値は設定できません。

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、RIP ルート集約をディセーブルにする例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

次に、自動 EIGRP ルート集約をディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての **router** コマンドとルータ コンフィギュレーション モード コマンドをクリアします。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、EIGRP ルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。
show running-config router	実行コンフィギュレーション内の **router** コマンドとルータ コンフィギュレーション モード コマンドを表示します。

auto-update device-id

Auto Update Server で使用するセキュリティ アプライアンスのデバイス ID を設定するには、グローバル コンフィギュレーション モードで **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

構文の説明

hardware-serial	セキュリティ アプライアンスのハードウェア シリアル番号を使用して、デバイスを一意に識別します。
hostname	セキュリティ アプライアンスのホスト名を使用して、デバイスを一意に識別します。
ipaddress [*if_name*]	セキュリティ アプライアンスの IP アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。
mac-address [*if_name*]	セキュリティ アプライアンスの MAC アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。
string *text*	テキスト ストリングを指定して、デバイスを Auto Update Server に対して一意に識別します。

デフォルト

デフォルト ID はホスト名です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、デバイス ID をシリアル番号に設定する例を示します。

```
hostname(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	Auto Update Server からのアップデートをセキュリティ アプライアンスが確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-at

セキュリティ アプライアンスが Auto Update Server をポーリングする特定の日時をスケジューリングするには、グローバル コンフィギュレーション モードで **auto-update poll-at** コマンドを使用します。セキュリティ アプライアンスが Auto Update Server をポーリングするようにスケジューリングした日時のうち、指定した日時をすべて削除するには、このコマンドの **no** 形式を使用します。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

構文の説明

days-of-the-week	任意の 1 つの曜日（Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday）または曜日の組み合わせ。その他の指定可能な値は、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、および weekend（土曜日と日曜日）です。
randomize *minutes*	指定した開始日時の後、不定期にポーリングする期間を指定します。1 ～ 1439 分です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を指定します。デフォルトは 5 分です。指定できる範囲は 1 ～ 35791 分です。
time	ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は 8:00 AM で、20:00 は 8:00 PM です

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

auto-update poll-at コマンドでは、更新をポーリングする時刻を指定します。**randomize** オプションをイネーブルにすると、最初の *time* の時刻から指定した期間（分単位）内に、ポーリングが不定期に実行されます。**auto-update poll-at** および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次の例で、セキュリティ アプライアンスは、毎週金曜日と土曜日の午後 10 時から午後 11 時までの間、不定期に Auto Update Server を ポーリングします。セキュリティ アプライアンスは、サーバに接続できない場合、10 分間隔で 2 回接続を試行します。

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートをセキュリティ アプライアンスが確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	セキュリティ アプライアンスの内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-period

セキュリティ アプライアンスが Auto Update Server からの更新を確認する頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。パラメータをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

構文の説明

poll_period	Auto Update Server をポーリングする頻度を分単位（1 ～ 35791）で指定します。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を分単位（1 ～ 35791）で指定します。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング期間は、720 分（12 時間）です。

Auto Update Server への最初の接続試行に失敗した場合に再接続を試行するデフォルトの回数は 0 です。

接続試行のデフォルト間隔は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

auto-update poll-at および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次に、ポーリング期間を 360 分に、再試行回数を 1 回に、再試行間隔を 3 分に設定する例を示します。

```
hostname(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス デバイス ID を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update server

Auto Update Server を指定するには、グローバル コンフィギュレーション モードで **auto-update server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM の更新がないか調べます。

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

構文の説明

interface	要求を Auto Update Server に送信するときに使用するインターフェイスを指定します。
url	次の構文を使用して、Auto Update Server の場所を指定します。 **http**[**s**]**:**[[*user:password@*]*location* [*:port*]] / *pathname*
verify_certificate	Auto Update Server から返された証明書を検証します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	複数のサーバをサポートできるようにコマンドが変更されました。

使用上のガイドライン

自動更新用に複数のサーバを設定できます。更新を確認するときに、最初のサーバに接続しますが、接続に失敗した場合は、次のサーバに接続します。これは、すべてのサーバを試行するまで続行されます。どのサーバにも接続できなかった場合は、auto-update poll-period が接続を再試行するように設定されていれば、最初のサーバから順に接続が再試行されます。

自動更新機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。同様に、**asdm image** コマンドを使用して、自動更新で ASDM ソフトウェア イメージを更新する必要があります。

source *interface* 引数で指定されたインターフェイスが **management-access** コマンドで指定されたインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネルを介して送信されます。

例

次に、Auto Update Server の URL を設定し、インターフェイス outside を指定する例を示します。

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートをセキュリティ アプライアンスが確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	セキュリティ アプライアンスの内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update timeout

Auto Update Server へのアクセスのタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。タイムアウト期間内に Auto Update Server へのアクセスが行われなかった場合、セキュリティ アプライアンスはセキュリティ アプライアンスを通過するすべてのトラフィックを停止します。タイムアウトを設定すると、セキュリティ アプライアンスに最新のイメージとコンフィギュレーションが保持されます。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout *period*

no auto-update timeout [*period*]

構文の説明

period	タイムアウト期間を分単位（1 ～ 35791）で指定します。デフォルトは 0 で、タイムアウトがないことを意味します。タイムアウトを 0 に設定することはできません。タイムアウトを 0 にリセットするには、このコマンドの **no** 形式を使用します。

デフォルト

デフォルトのタイムアウトは 0 で、セキュリティ アプライアンスはタイムアウトしないように設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

タイムアウト状態は、システム ログ メッセージ 201008 でレポートされます。

例

次に、タイムアウトを 24 時間に設定する例を示します。

```
hostname(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server で使用するためのセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートをセキュリティ アプライアンスが確認する頻度を設定します。

auto-update server	Auto Update Server を指定します。
clear configure auto-update	Auto Update Server のコンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

CHAPTER 4

backup interface コマンド～ browse-networks コマンド

backup interface

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **backup interface** コマンドを使用して、ISP などのバックアップ インターフェイスとして VLAN インターフェイスを指定します。このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。このコマンドは、プライマリ インターフェイスを経由するデフォルト ルートがダウンしない限り、指定したバックアップ インターフェイスを通過しようとするトラフィックをすべてブロックします。通常の動作に戻すには、**no backup interface** コマンドを使用します。

backup interface vlan *number*

no backup interface vlan *number*

構文の説明

vlan *number*	バックアップ インターフェイスの VLAN ID を指定します。

デフォルト

デフォルトでは、**backup interface** コマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	Security Plus ライセンスでは、VLAN インターフェイス数の制限（通常のトラフィック用は 3 つ、バックアップ インターフェイス用は 1 つ、フェールオーバー用は 1 つ）がなくなり、最大 20 のインターフェイスを設定できるようになりました（最大数以外の制限はありません）。したがって、4 つ以上のインターフェイスをイネーブルにするために **backup interface** コマンドを使用する必要がなくなりました。

使用上のガイドライン

backup interface コマンドで Easy VPN を設定した場合は、バックアップ インターフェイスがプライマリになると、セキュリティ アプライアンスは VPN ルールを新しいプライマリ インターフェイスに移動します。バックアップ インターフェイスの状態を表示する方法については、**show interface** コマンドを参照してください。

必ずプライマリ インターフェイスとバックアップ インターフェイスの両方にデフォルト ルートを設定して、プライマリ インターフェイスに障害が発生した場合にバックアップ インターフェイスを使用できるようにしてください。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。DHCP サーバから取得

したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きする方法については、**dhcp client route distance** コマンドを参照してください。デュアル ISP サポートの設定の詳細については、**sla monitor** コマンドおよび **track rtr** コマンドを参照してください。

management-only コマンドをすでに設定しているインターフェイスをバックアップ インターフェイスに設定することはできません。

例

次に、4 つの VLAN インターフェイスを設定する例を示します。backup-isp インターフェイスは、プライマリ インターフェイスがダウンしている場合に限り、通過トラフィックを許可します。**route** コマンドでは、プライマリ インターフェイスとバックアップ インターフェイスのデフォルト ルートを作成し、バックアップ ルートには低いアドミニストレーティブ ディスタンスを設定しています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# backup interface vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# route outside 0 0 10.1.1.2 1
hostname(config)# route backup-isp 0 0 10.1.2.2 2
```

関連コマンド

コマンド	説明
forward interface	インターフェイスが別のインターフェイスへのトラフィックを開始することを制限します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
dhcp client route distance	DHCP サーバから取得したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きします。
sla monitor	スタティック ルートのトラッキングの SLA モニタリング動作を作成します。
track rtr	SLA モニタリング動作の状態を追跡します。

backup-servers

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを使用します。バックアップ サーバを削除するには、このコマンドの **no** 形式を使用します。実行コンフィギュレーションから backup-servers 属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。これにより、backup-servers の値を別のグループ ポリシーから継承できます。

IPSec バックアップ サーバにより、VPN クライアントは、プライマリセキュリティ アプライアンスが利用できない場合でも中央サイトに接続できます。バックアップ サーバを設定すると、IPSec トンネルが確立されるときにセキュリティ アプライアンスがクライアントにサーバ リストをプッシュします。

backup-servers {*server1 server2. . . . server10* | **clear-client-config | keep-client-config}**

no backup-servers [*server1 server2. . . . server10* | **clear-client-config | keep-client-config**]

構文の説明

clear-client-config	クライアントがバックアップ サーバを使用しないことを指定します。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。
keep-client-config	セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。
server1 server 2....server10	プライマリセキュリティ アプライアンスが利用できない場合に VPN クライアントが使用するサーバのリストを指定します。各サーバをスペースで区切り、プライオリティの高い順に並べます。サーバは、IP アドレスまたはホスト名で指定します。リストには 500 文字まで入力できますが、10 個のエントリのみを含めることができます。

デフォルト

クライアント上またはプライマリセキュリティ アプライアンス上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

バックアップ サーバは、クライアント上またはプライマリセキュリティ アプライアンス上に設定します。セキュリティ アプライアンス上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。さらに、ホスト名を使用するときに DNS サーバが利用できないと、重大な遅延が発生することがあります。

例

次に、「FirstGroup」という名前のグループ ポリシーに IP アドレス 10.10.10.1 および 192.168.10.14 のバックアップ サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

ASDM バナー、セッション バナー、ログイン バナー、または Message-of-The-Day バナーを設定するには、グローバル コンフィギュレーション モードで **banner** コマンドを使用します。**no banner** コマンドは、指定したバナー キーワード（**exec**、**login**、または **motd**）のすべての行を削除します。

banner {**asdm** | **exec** | **login** | **motd** *text*}

[no] banner {**asdm** | **exec** | **login** | **motd** [*text*]}

構文の説明

asdm	ASDM へのログインに成功した後にバナーを表示するようにシステムを設定します。続行してログインを完了するか、または切断するかを確認するプロンプトがユーザに表示されます。このオプションを使用すると、接続の前に、書面によるポリシー条件の受け入れをユーザに求めることができます。
exec	イネーブル プロンプトを表示する前に、バナーを表示するようにシステムを設定します。
login	Telnet を使用してセキュリティ アプライアンスにアクセスする場合、パスワード ログイン プロンプトを表示する前にバナーを表示するようにシステムを設定します。
motd	初めて接続したときに Message-of-The-Day バナーを表示するようにシステムを設定します。
text	表示するメッセージ テキスト行。

デフォルト

デフォルトでは、バナーは表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(4)/8.0(3)	**asdm** キーワードが追加されました。

使用上のガイドライン

banner コマンドは、指定したキーワードに対応して表示されるようにバナーを設定します。*text* ストリングは、最初の空白（スペース）の後に続く、行末（復帰または改行（LF））までのすべての文字で構成されます。テキスト内のスペースは維持されます。ただし、CLI ではタブを入力できません。

最初に既存のバナーをクリアしない限り、後続の *text* エントリは既存のバナーの末尾に追加されていきます。

（注）　$(domain) トークンと $(hostname) トークンは、セキュリティ アプライアンスのドメイン名とホスト名にそれぞれ置き換えられます。コンテキスト コンフィギュレーションで $(system) トークンを入力すると、このコンテキストでは、システム コンフィギュレーションで設定されているバナーが使用されます。

バナーを複数行にするには、追加する行ごとに banner コマンドを新たに入力します。各行は、既存のバナーの末尾に追加されていきます。RAM およびフラッシュでの制限を除き、バナーの長さに制限はありません。

Telnet または SSH を介してセキュリティ アプライアンスにアクセスする場合は、バナー メッセージの処理に必要なシステム メモリが十分ないか、または TCP 書き込みエラーが発生すると、セッションが閉じます。exec バナーと motd バナーだけが、SSH を介したセキュリティ アプライアンスへのアクセスをサポートしています。login バナーは SSH をサポートしていません。

バナーを置き換えるには、**no banner** コマンドを使用してから、新しい行を追加します。

指定したバナー キーワードのすべての行を削除するには、**no banner** {**exec | login | motd**} コマンドを使用します。

no banner コマンドでは、テキスト ストリングを選択して削除することはできません。そのため、**no banner** コマンドの末尾に入力したテキストはすべて無視されます。

例

次に、**asdm**、**exec**、**login**、および **motd** の各バナーを設定する例を示します。

```
hostname(config)# banner asdm You successfully logged in to ASDM
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

次に、**motd** バナーに別の行を追加する例を示します。

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

関連コマンド

コマンド	説明
clear configure banner	すべてのバナーを削除します。
show running-config banner	すべてのバナーを表示します。

banner（グループ ポリシー）

リモート クライアントの接続時にリモート クライアント上でバナー（ウェルカム テキスト）を表示するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを使用します。バナーを削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーのバナーを継承できます。バナーを継承しないようにするには、**banner none** コマンドを使用します。

banner {**value** *banner_string* | **none**}

no banner

（注）　VPN グループ ポリシーで複数のバナーを設定し、いずれかのバナーを削除すると、すべてのバナーが削除されます。

構文の説明

none	バナーにヌル値を設定して、バナーを禁止します。デフォルトまたは指定したグループ ポリシーのバナーを継承しません。
value *banner_string*	バナー テキストを設定します。最大ストリング サイズは 500 文字です。復帰を挿入するには、「\n」シーケンスを使用します。

デフォルト

デフォルトのバナーはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレス ポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモート ユーザに適切に表示されるようにするには、次のガイドラインに従います。

- IPsec クライアント ユーザの場合は、/n タグを使用します。
- AnyConnect クライアント ユーザの場合は、
 タグを使用します。
- クライアントレス ユーザの場合は、
 タグを使用します。

例

次に、「FirstGroup」という名前のグループ ポリシー用のバナーを作成する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、特権 EXEC モードで **blocks** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50% を超えることはありません。必要に応じて、メモリ サイズを手動で指定できます。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

構文の説明

memory_size	（任意）ダイナミックな値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50% を超える場合は、警告メッセージが表示されますが、値は受け入れられます。

デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは、2136 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

セキュリティ アプライアンスをリロードすると、メモリ割り当てがデフォルトに戻ります。

例

次に、ブロック診断用のメモリ サイズを増やす例を示します。

```
hostname# blocks queue history enable
```

次に、メモリ サイズを 3000 バイトに増やす例を示します。

```
hostname# blocks queue history enable 3000
```

次に、メモリ サイズを 3000 バイトに増やすことを試みるものの、この値が空きメモリを超えている例を示します。

```
hostname# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次に、メモリ サイズを 3000 バイトに増やすものの、この値が空きメモリの 50% を超えている例を示します。

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

関連コマンド

コマンド	説明
clear blocks	システム バッファの統計情報をクリアします。
show blocks	システム バッファの使用状況を表示します。

boot

システムが次回のリロードで使用するシステム イメージ、およびシステムが起動時に使用するコンフィギュレーション ファイルを指定するには、グローバル コンフィギュレーション モードで **boot** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

構文の説明

config	システムがロードされるときに使用するコンフィギュレーション ファイルを指定します。
system	システムがロードされるときに使用するシステム イメージ ファイルを指定します。
url	イメージまたはコンフィギュレーションの場所を設定します。マルチ コンテキスト モードでは、管理コンテキストですべてのリモート URL にアクセスできる必要があります。次の URL 構文を参照してください。 • **disk0:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。 • **flash:**/[*path*/]*filename* この URL は内部フラッシュ メモリを示します。 • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスの **boot system** コマンドだけで使用できます。**boot config** コマンドを使用するには、スタートアップ コンフィギュレーションがフラッシュ メモリに存在している必要があります。 **boot system tftp:** コマンドは、1 つのみ設定でき、かつ最初に設定する必要があります。

デフォルト

boot config コマンドを指定しないと、スタートアップ コンフィギュレーションが非表示の場所に保存され、スタートアップ コンフィギュレーションを利用するコマンド（**show startup-config** コマンドや **copy startup-config** コマンド）だけで使用されるようになります。

boot system コマンドにデフォルトはありません。場所を指定しないと、セキュリティ アプライアンスは、ブートする最初の有効なイメージを内部フラッシュ メモリでのみ探します。有効なイメージが見つからない場合は、システム イメージがロードされず、セキュリティ アプライアンスは、ROMMON モードまたはモニタ モードが開始されるまでブート ループ状態になります。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、BOOT 環境変数と CONFIG_FILE 環境変数にも設定が保存されます。セキュリティ アプライアンスは、これらの環境変数を使用して、再起動時のスタートアップ コンフィギュレーションおよびブートするソフトウェア イメージを決定します。

最大 4 つの **boot system** コマンド エントリを入力して異なるイメージを指定し、順番にブートすることができます。セキュリティ アプライアンスは、最初に見つけた有効なイメージをブートします。

現在の実行コンフィギュレーションとは異なる、新しい場所にあるスタートアップ コンフィギュレーション ファイルを使用する場合は、実行コンフィギュレーションを保存した後に、必ず、スタートアップ コンフィギュレーション ファイルを新しい場所にコピーしてください。このようにしないと、実行コンフィギュレーションの保存時に、実行コンフィギュレーションによって新しいスタートアップ コンフィギュレーションが上書きされます。

ヒント　ASDM イメージ ファイルは、**asdm image** コマンドで指定します。

例　次に、起動時にセキュリティ アプライアンスが configuration.txt という名前のコンフィギュレーション ファイルをロードするように指定する例を示します。

```
hostname(config)# boot config disk0:/configuration.txt
```

関連コマンド

コマンド	説明
asdm image	ASDM ソフトウェア イメージを指定します。
show bootvar	ブート ファイルおよびコンフィギュレーションの環境変数を表示します。

border style

認証された WebVPN ユーザに表示される WebVPN ホームページの境界線をカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **border style** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

border style *value*

no border style *value*

構文の説明

value	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータ（最大 256 文字）。

デフォルト

境界線のデフォルト スタイルは background-color:#669999;color:white です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、境界線の背景色を RGB カラー #66FFFF（緑色の一種）にカスタマイズする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# border style background-color:66FFFF
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

browse-networks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Browse Networks] ボックスをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **browse-networks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

構文の説明

dropdown	ドロップダウン リストを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
title	タイトルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

タイトルのデフォルト テキストは「Browse Networks」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

メッセージのデフォルト テキストは「Enter Network Path」です。

メッセージのデフォルト スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

ドロップダウンのデフォルト テキストは「File Folder Bookmarks」です。

ドロップダウンのデフォルト スタイルは次のとおりです。

border:1px solid black;font-weight:bold;color:black;font-size:80%.

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Browse Corporate Networks」に変更し、スタイル内のテキストを青色に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
F1-asa1(config-webvpn-custom)# browse-networks title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

CHAPTER 5

cache コマンド～ clear compression コマンド

cache

キャッシュ モードを開始し、キャッシング属性の値を設定するには、webvpn コンフィギュレーション モードで **cache** コマンドを入力します。コンフィギュレーションからキャッシュ関連のコマンドをすべて削除し、これらをデフォルト値にリセットするには、このコマンドの **no** 形式を入力します。

cache

no cache

デフォルト

各キャッシュ属性のデフォルト設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシュ モードを開始する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache-static-content	書き換えの対象でないコンテンツをキャッシュします。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

cache-fs limit

セキュリティ アプライアンスがリモート PC にダウンロードするイメージを保存するために使用するキャッシュ ファイル システムのサイズを制限するには、webvpn コンフィギュレーション モードで **cache-fs limit** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cache-fs limit {*size*}

no cache-fs limit {*size*}

構文の説明

size	キャッシュ ファイル システムのサイズ制限（1 ～ 32 MB）。

デフォルト

デフォルト値は 20 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、Cisco AnyConnect VPN Client および Cisco Secure Desktop（CSD）のイメージおよびファイルを含むパッケージ ファイルを、リモート PC へのダウンロード用にキャッシュ メモリ内で展開します。セキュリティ アプライアンスで正常にパッケージ ファイルを展開するには、このイメージとファイルを保存するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことをセキュリティ アプライアンスが検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドで AnyConnect VPN Client のイメージ パッケージをインストールしようとした後にレポートされるエラー メッセージの例を示します。

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

イメージ パッケージをインストールしようとしてこのエラー メッセージがレポートされた場合は、グローバル コンフィギュレーション モードで **dir cache:/** コマンドを使用して、キャッシュ メモリの残量およびこれまでにインストールしたパッケージのサイズを検査できます。検査結果に応じて、キャッシュ サイズの制限を調整できます。

例

次に、CSD イメージ（sdesktop 内）および CVC イメージ（stc 内）が約 5.44 MB のキャッシュ メモリを使用している例を示します。

```
hostname(config-webvpn)# dir cache:/

Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)
```

次に、キャッシュ サイズを 6 MB に制限する例を示します。

```
hostname(config-webvpn)# cache-fs limit 6
```

関連コマンド

コマンド	説明
dir cache:/	キャッシュ メモリの内容（予約されているキャッシュ メモリの総量やキャッシュ メモリの残量など）を表示します。
show run webvpn	現在の WebVPN コンフィギュレーション（キャッシュ メモリを消費する可能性があるインストール済みの SSL VPN クライアントや CSD イメージなど）を表示します。
show webvpn csd	CSD バージョンおよびインストール ステータスを表示します。
show webvpn svc	インストール済みの SSL VPN パッケージ ファイルの名前およびバージョンを表示します。

cache-static-content

クライアントレス SSL VPN 接続に使用するすべての静的コンテンツがキャッシュ メモリにロードされるようセキュリティ アプライアンスを設定するには、キャッシュ コンフィギュレーション モードで **cache-static-content** コマンドを使用します。

cache-static-content enable

no cache-static-content enable

構文の説明

enable	すべての静的コンテンツのキャッシュ メモリへのロードをイネーブルにします。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn キャッシュ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

キャッシュ可能なすべての静的コンテンツがセキュリティ アプライアンスのキャッシュに保存されるようセキュリティ アプライアンスを設定すると、バックエンド SSL VPN 接続のパフォーマンスが向上します。静的コンテンツには、PDF ファイルやイメージなど、セキュリティ アプライアンスによってデータの書き換え（上書き）が行われないオブジェクトが含まれています。

例

次の例は、静的コンテンツのキャッシュをイネーブルにする方法を示したものです。

```
hostname(config-webvpn-cache)# cache-static-content enable
```

関連コマンド

コマンド	説明
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。

cache-time

CRL を失効と見なす前にキャッシュ内に残す時間を分単位で指定するには、crl 設定コンフィギュレーション モードで **cache-time** コマンドを使用します。このモードには、クリプト CA トラストポイント コンフィギュレーション モードからアクセスできます。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cache-time *refresh-time*

no cache-time

構文の説明

refresh-time	CRL をキャッシュ内に残す時間を分単位で指定します。指定できる範囲は 1 ～ 1440 分です。CRL に NextUpdate フィールドがない場合、CRL はキャッシュされません。

デフォルト

デフォルトの設定は 60 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central でキャッシュ時間のリフレッシュ値を 10 分に指定する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
enforcenextupdate	証明書で NextUpdate CRL フィールドを処理する方法を指定します。

call-agent

コール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドを使用します。このモードには、**mgcp-map** コマンドを使用してアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

構文の説明

ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 つ以上のゲートウェイを管理できるコール エージェントのグループを指定するには、**call-agent** コマンドを使用します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ *group_id* を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。*group_id* オプションには、0 ～ 4294967295 の数字を指定します。*ip_address* オプションには、コール エージェントの IP アドレスを指定します。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
```

```
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

call-duration-limit

H.323 コールのコール継続時間を設定するには、パラメータ コンフィギュレーション モードで **call-duration-limit** コマンドを使用します。このモードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

構文の説明

hh:mm:ss	継続時間を時、分、および秒で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 コールのコール継続時間を設定する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-duration-limit 0:1:0
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

call-party-numbers

H.323 コールの設定時に発信側の番号の送信を適用にするには、パラメータ コンフィギュレーション モードで **call-party-numbers** コマンドを使用します。このモードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-party-numbers

no call-party-numbers

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 コールのコール設定時に発信側の番号を適用する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-party-numbers
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

capture

パケット キャプチャ機能をイネーブルにして、パケットのスニッフィングやネットワーク障害を検出できるようにするには、特権 EXEC モードで **capture** コマンドを使用します。パケット キャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

capture *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy**| **raw-data** | **isakmp** | **decrypted** | **webvpn user** *webvpn-user* [**url** *url*]}] [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

no capture *capture-name* [**type** {**asp-drop** [*drop-code*] | **tls-proxy** | **raw-data** | **isakmp** | **decrypted** | **webvpn user** *webvpn-user*] [**access-list** *access_list_name*] [**circular-buffer**] [**interface** *interface_name*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot*] {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

構文の説明

access-list *access_list_name*	（任意）アクセス リストと一致するトラフィックをキャプチャします。マルチ コンテキスト モードでは、1 つのコンテキスト内でのみこのコマンドを使用できます。
any	単一の IP アドレスおよびマスクではなく、任意の IP アドレスを指定します。
all	セキュリティ アプライアンスがドロップするパケットをすべてキャプチャします。
asp-drop [*drop-code*]	（任意）高速セキュリティ パスでドロップされるパケットをキャプチャします。*drop-code* は、高速セキュリティ パスでドロップされるトラフィックのタイプを指定します。ドロップ コードのリストについては、**show asp drop frame** コマンドを参照してください。*drop-code* 引数を入力しないと、ドロップされるパケットすべてがキャプチャされます。 このキーワードは、**packet-length**、**circular-buffer**、および **buffer** とともに入力できますが、**interface** または **ethernet-type** とともには入力できません。
buffer *buf_size*	（任意）パケットの保存に使用するバッファのサイズをバイト単位で定義します。このバイト数のバッファがいっぱいになると、パケット キャプチャは停止します。
capture_name	パケット キャプチャの名前を指定します。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ名前を使用します。**show capture** コマンドを使用してキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめられます。
circular-buffer	（任意）バッファがいっぱいになったとき、バッファを先頭から上書きします。
detail	（任意）各パケットについて、プロトコル情報を追加表示します。
dump	（任意）データ リンク トランスポート経由で転送されたパケットの 16 進ダンプを表示します。
decrypted	（任意）復号化 TCP データは、L2-L4 ヘッダーでカプセル化され、キャプチャ エンジンによってキャプチャされます。
ethernet-type *type*	（任意）キャプチャするイーサネット タイプを選択します。デフォルトは IP パケットです。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。
host *ip*	パケット送信先ホストの単一の IP アドレスを指定します。

interface *interface_name*	パケット キャプチャを使用するインターフェイスの名前を設定します。キャプチャするすべてのパケットのインターフェイスを設定する必要があります。複数の **capture** コマンドで同じ名前を使用して、複数のインターフェイスを設定できます。ASA 5500 シリーズ適応型セキュリティ アプライアンスのデータプレーン上のパケットをキャプチャするには、**interface** キーワードとともにインターフェイスの名前として **asa_dataplane** を使用できます。
isakmp	（任意）ISAKMP トラフィックをキャプチャします。これは、マルチ コンテキスト モードでは使用できません。ISAKMP サブシステムは、上位層プロトコルにアクセスできません。このキャプチャは、PCAP パーサーを満たすために物理層、IP レイヤ、および UDP レイヤを組み合わせた疑似キャプチャです。このピア アドレスは、SA 交換から取得され、IP レイヤに保存されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定する場合に使用する方式は、Cisco IOS ソフトウェア **access-list** コマンドの方式と異なります。このセキュリティ アプライアンスは、ネットワーク マスク（たとえば、クラス C マスクの場合は 255.255.255.0）を使用します。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。
match *prot*	5 タプルが一致するパケットを指定し、キャプチャされるこれらのパケットのフィルタリングを許可します。1 行に最大 3 回このキーワードを使用できます。
operator	（任意）送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい
packet-length *bytes*	（任意）キャプチャ バッファに保存する各パケットの最大バイト数を設定します。
port	（任意）プロトコルを **tcp** または **udp** に設定する場合、TCP ポートまたは UDP ポートの番号（整数）か名前を指定します。
raw-data	（任意）着信パケットおよび発信パケットを 1 つ以上のインターフェイスでキャプチャします。この設定は、デフォルトです。
real-time	キャプチャしたパケットをリアルタイムで継続的に表示します。リアルタイムのパケット キャプチャを終了するには、**Ctrl+C** を押します。このオプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにだけ適用されます。
tls-proxy	（任意）1 つ以上のインターフェイスで TLS プロキシからの復号化されたインバウンド データおよびアウトバウンド データをキャプチャします。
trace *trace_count*	（任意）パケット トレース情報、およびキャプチャするパケット数をキャプチャします。これは、アクセス リストとともに使用され、トレース パケットをデータ パスに挿入して、パケットが想定どおりに処理されているかどうかを判別します。
type	（任意）キャプチャされるデータのタイプを指定します。
url *url*	（任意）データのキャプチャのために照合する URL プレフィックスを指定します。サーバへの HTTP トラフィックをキャプチャするには、URL の形式として http://*server*/*path* を使用します。サーバへの HTTPS トラフィックをキャプチャするには、https://*server*/*path* を使用します。
user *webvpn-user*	（任意）WebVPN キャプチャのユーザ名を指定します。
webvpn	（任意）特定の WebVPN 接続の WebVPN データをキャプチャします。

デフォルト

デフォルトの設定は次のとおりです。

- デフォルトの **type** は **raw-data** です。
- デフォルトの **buffer** *size* は 512 KB です。
- デフォルトのイーサネット タイプは IP です。
- デフォルトの **packet-length** は 1518 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
6.2(1)	このコマンドが導入されました。
7.0(1)	キーワード **type asp-drop**、**type isakmp**、**type raw-data**、および **type webvpn** を含むように変更されました。
7.0(8)	セキュリティ アプライアンスがドロップするパケットをすべてキャプチャするように、**all** オプションが追加されました。
7.2(1)	オプション **trace** *trace_count*、**match** *prot*、**real-time**、**host** *ip*、**any**、*mask*、および *operator* を含むように変更されました。
8.0(2)	キャプチャした内容にパスを更新するように変更されました。
8.0(4)	キーワード **type decrypted** を含むように変更されました。

使用上のガイドライン

パケット キャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立ちます。複数のキャプチャを作成できます。パケット キャプチャを表示するには、**show capture** *name* コマンドを使用します。キャプチャをファイルに保存するには、**copy capture** コマンドを使用します。パケット キャプチャ情報を Web ブラウザで表示するには、**https://** *セキュリティ アプライアンス-ip-address*/*admin*/**capture**/*capture_name*[/**pcap**] コマンドを使用します。オプションの **pcap** キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされ、Web ブラウザを使用してこのファイルを保存できます（libcap ファイルは、TCPDUMP または Ethereal で表示できます）。

バッファの内容を TFTP サーバに ASCII 形式でコピーする場合、パケットの詳細および 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細および 16 進ダンプを表示するには、バッファを PCAP 形式で転送し、TCPDUMP または Ethereal で読み取る必要があります。

（注） WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成した後、必ずキャプチャをディセーブルにしてください。

オプションのキーワードを指定せずに **no capture** を入力すると、キャプチャが削除されます。オプションの **access-list** キーワードを指定すると、このアクセス リストがキャプチャから削除され、キャプチャは保持されます。**interface** キーワードを指定すると、指定したインターフェイスからキャプチャが分離され、キャプチャは保持されます。キャプチャ自体をクリアしない場合は、**no capture** コマンドをオプションの **access-list** キーワードまたは **interface** キーワードのいずれかを指定して入力します。

リアルタイム表示の進行中には、キャプチャに関するあらゆる操作を実行できません。低速のコンソール接続で **real-time** キーワードを使用すると、パフォーマンスが考慮されて、多数のパケットが非表示になる場合があります。バッファの固定の制限は、1000 パケットです。バッファがいっぱいになると、カウンタはキャプチャしたパケットで維持されます。別のセッションを開く場合、**no capture real-time** コマンドを入力して、リアルタイム表示をディセーブルにできます。

（注） **capture** コマンドは、コンフィギュレーションには保存されません。また、フェールオーバー時にスタンバイ ユニットにコピーされません。

例

パケットをキャプチャするには、次のコマンドを入力します。

```
hostname# capture captest interface inside
hostname# capture captest interface outside
```

Web ブラウザ上で、発行された capture コマンドの内容（「captest」という名前）は、次の場所に表示できます。

```
https://171.69.38.95/admin/capture/captest
```

libpcap ファイル（Web ブラウザが使用）をローカル マシンにダウンロードするには、次のコマンドを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次に、外部ホスト 171.71.69.234 から内部 HTTP サーバにトラフィックがキャプチャされる例を示します。

```
hostname# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname# capture http access-list http packet-length 74 interface inside
```

次に、ARP パケットをキャプチャする例を示します。

```
hostname# capture arp ethernet-type arp interface outside
```

次に、5 つのトレース パケットをデータ ストリームに挿入する例を示します。ここで、*access-list 101* は、TCP プロトコル FTP と一致するトラフィックを定義します。

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

トレースされたパケットおよびパケット処理に関する情報をわかりやすく表示するには、**show capture ftptrace** コマンドを使用します。

次に、キャプチャしたパケットをリアルタイムで表示する例を示します。

```
hostname# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

関連コマンド

コマンド	説明
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

cd

現在の作業ディレクトリから指定したディレクトリに変更するには、特権 EXEC モードで **cd** コマンドを使用します。

cd [**disk0: | disk1: | flash:**] [*path*]

構文の説明

disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	取り外し可能な外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）移動先ディレクトリの絶対パス。

デフォルト

ディレクトリを指定しないと、ルート ディレクトリに移動します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「config」ディレクトリに移動する例を示します。

```
hostname# cd flash:/config/
```

関連コマンド

コマンド	説明
pwd	現在の作業ディレクトリを表示します。

cdp-url

ローカル CA によって発行された証明書に含める CDP を指定するには、CA サーバ コンフィギュレーション モードで **cdp-url** コマンドを使用します。デフォルトの CDP に戻すには、このコマンドの **no** 形式を使用します。

[no] cdp-url *url*

構文の説明

url	ローカル CA によって発行された証明書の失効ステータスを検証側が取得する URL を指定します。URL は、英数字 500 文字未満である必要があります。

デフォルト

デフォルトの CDP URL は、ローカル CA が含まれるセキュリティ アプライアンスの CDP URL です。デフォルトの URL の形式は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CDP は、発行された証明書に含めることができる拡張であり、証明書の失効ステータスを検証側が取得できる場所を指定できます。一度に設定できる CDP は 1 つだけです。

（注） CDP URL が指定された場合、管理者はその場所から現在の CRL にアクセスできるように管理する必要があります。

例

次に、ローカル CA サーバが発行した証明書に対して、10.10.10.12 の CDP を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	証明書データベースおよび CRL で、ローカル CA サーバによって発行された証明書を失効とマークします。
crypto ca server unrevoke	ローカル CA サーバによって発行され、以前に失効した証明書の失効を取り消します。
lifetime crl	証明書失効リストのライフタイムを指定します。

certificate

指定した証明書を追加するには、クリプト CA 証明書チェーン コンフィギュレーション モードで **certificate** コマンドを使用します。このコマンドを発行する場合、セキュリティ アプライアンスは、コマンドに含まれているデータを 16 進形式の証明書として解釈します。**quit** ストリングは、証明書の末尾を示します。証明書を削除するには、このコマンドの **no** 形式を使用します。

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

構文の説明

certificate-serial-number	証明書のシリアル番号を quit で終わる 16 進形式で指定します。
ca	証明書が CA 発行の証明書であることを示します。
ra-encrypt	証明書が SCEP で使用される RA キー暗号化証明書であることを示します。
ra-general	証明書が SCEP メッセージングのデジタル署名およびキー暗号化に使用される RA 証明書であることを示します。
ra-sign	証明書が SCEP メッセージングで使用される RA デジタル署名証明書であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA 証明書チェーン コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

CA は、メッセージ暗号化のためのセキュリティ クレデンシャルおよび公開キーの発行および管理を行うネットワーク内の組織です。公開キー インフラストラクチャの一部である CA では、RA と連携して、デジタル証明書の要求者から取得した情報を確認します。RA が要求者の情報を確認すると、CA から証明書が発行されます。

例

次に、シリアル番号 29573D5FF010FE25B45 の CA 証明書を追加する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
```

```
0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
BEA3C1FE 5EE2AB6D 91
quit
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
crypto ca certificate chain	証明書クリプト CA 証明書チェーン モードを開始します。
crypto ca trustpoint	CA トラストポイント モードを開始します。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

certificate-group-map

証明書マップのルール エントリをトンネル グループに関連付けるには、webvpn コンフィギュレーション モードで **certificate-group-map** コマンドを使用します。現在のトンネル グループ マップの関連付けをクリアするには、このコマンドの **no** 形式を使用します。

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

構文の説明

certificate_map_name	証明書マップの名前。
index	証明書マップのマップ エントリの数値識別子。index の値の範囲は、1 ～ 65535 です。
tunnel_group_name	マップ エントリが証明書と一致する場合に選択されるトンネル グループの名前。*tunnel-group name* はすでに存在している必要があります。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

certificate-group-map コマンドが有効な状態で、WebVPN クライアントから受信した証明書がマップ エントリに対応する場合、結果として得られるトンネル グループは、接続に関連付けられ、ユーザが選択したトンネル グループを上書きします。

certificate-group-map コマンドの複数のインスタンスを使用すると、複数のマッピングが可能です。

例

次に、tgl という名前のトンネル グループにルール 6 を関連付ける例を示します。

```
hostname(config)# webvpn

hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	証明書の発行者名とサブジェクト Distinguished Name（DN; 認定者名）に基づいて、ルールを設定するために CA 証明書マップ コンフィギュレーション モードを開始します。
tunnel-group-map	証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。

chain

証明書チェーンの送信をイネーブルにするには、トンネル グループ ipsec 属性コンフィギュレーション モードで **chain** コマンドを使用します。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

chain

no chain

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

例

次に、トンネル グループ ipsec 属性コンフィギュレーション モードを開始し、IPSec LAN-to-LAN トンネル グループのチェーンを IP アドレス 209.165.200.225 で送信することをイネーブルにする例を示します。このアクションには、ルート証明書およびすべての下位 CA 証明書が含まれます。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

changeto

セキュリティ コンテキストとシステムの間で切り替えを行うには、特権 EXEC モードで **changeto** コマンドを使用します。

changeto {**system** | **context** *name*}

構文の説明

context *name*	指定した名前のコンテキストに切り替えます。
system	システム実行スペースに切り替えます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

システム実行スペースまたは管理コンテキストにログインしている場合、コンテキスト間で切り替えを行うことができ、各コンテキスト内でコンフィギュレーションおよびタスクのモニタリングを実行できます。コンフィギュレーション モードでの編集または **copy** コマンドあるいは **write** コマンドで使用される「実行」コンフィギュレーションは、ログインしている実行スペースによって異なります。システム実行スペースにログインしている場合、実行コンフィギュレーションは、システム コンフィギュレーションのみで構成されます。コンテキスト実行スペースにログインしている場合、実行コンフィギュレーションは、このコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

例

次に、特権 EXEC モードでコンテキストとシステムの間で切り替えを行う例を示します。

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

次に、インターフェイス コンフィギュレーション モードでシステムと管理コンテキストの間で切り替えを行う例を示します。実行スペース間で切り替えを行うときにコンフィギュレーション サブモードにログインしている場合、新しい実行スペースのグローバル コンフィギュレーション モードに変更されます。

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

関連コマンド

コマンド	説明
admin-context	コンテキストを管理コンテキストに設定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

character-encoding

WebVPN ポータル ページでグローバルな文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **character-encoding** コマンドを使用します。character-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

character-encoding *charset*

no character-encoding [*charset*]

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンス コンフィギュレーション内では、コマンド インタプリタによって大文字が小文字に変換されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

文字エンコーディング（「文字コーディング」または「文字セット」とも呼ばれます）は、raw データ（0 と 1 からなるデータなど）と文字をペアにすることで、データを表します。使用する文字エンコード方式は、言語によって決まります。ある言語では同じ方式を使用していても、別の言語でも同じとはかぎりません。通常、ブラウザで使用されるデフォルトのエンコーディング方式は地域によって決まりますが、ユーザはこの方式を変更できます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。character-encoding 属性を使用すると、ユーザは、文字エンコーディング方式の値を WebVPN ポータル ページに指定し、ブラウザを使用している地域やブラウザに対して行われたあらゆる変更に関係なく、ブラウザでこのページを適切に処理できます。

character-encoding 属性は、デフォルトでは、すべての WebVPN ポータル ページに継承されるグローバルな設定です。ただし、ユーザは、character-encoding 属性の値と異なる文字エンコーディングを使用する Common Internet File System サーバの file-encoding 属性を上書きできます。異なる文字エンコーディングが必要な CIFS サーバには異なるファイル エンコーディング値を使用します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding 属性の値を符号化します。符号化が行われなかった場合は、character-encoding 属性の値を継承します。リモート ユーザのブラウザでは、ブラウザの文字エンコード セットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding 属性によって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注）　character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。Shift_JIS 文字エンコーディングを使用している場合、次の例に示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用して、これらの値の 1 つの設定を補完して、フォント ファミリを置き換える必要があります。あるいは、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力して、このフォント ファミリを削除する必要があります。

この属性に値が含まれていない場合、WebVPN ポータル ページの文字セットは、リモート ブラウザに設定されているエンコーディング タイプによって決まります。

例

次に、日本語 Shift_JIS 文字をサポートする character-encoding 属性を設定し、フォント ファミリを削除し、デフォルトの背景色を保持する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

関連コマンド

コマンド	説明
file-encoding	CIFS サーバおよび関連する文字エンコーディングを指定し、この属性の値を上書きします。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。

checkheaps

checkheaps 検証の間隔を設定するには、グローバル コンフィギュレーション モードで **checkheaps** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

checkheaps {check-interval | **validate-checksum}** *seconds*

no checkheaps {check-interval | **validate-checksum}** [*seconds*]

構文の説明

check-interval	バッファ検証の間隔を設定します。バッファ検証プロセスでは、ヒープ（割り当てられ、解放されたメモリ バッファ）の健全性がチェックされます。このプロセスの各呼び出しの間、セキュリティ アプライアンスはヒープ全体をチェックし、各メモリ バッファを検証します。不一致がある場合、セキュリティ アプライアンスは、「バッファ割り当てエラー」または「バッファ解放エラー」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
validate-checksum	コード スペースのチェックサム検証間隔を設定します。最初にセキュリティ アプライアンスを起動するときに、セキュリティ アプライアンスはコード全体のハッシュを計算します。その後、セキュリティ アプライアンスは、定期チェックの間に新しいハッシュを生成し、元のハッシュと比較します。不一致がある場合、セキュリティ アプライアンスは「テキスト チェックサム checkheaps エラー」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
seconds	1 ～ 2147483 の間隔を秒単位で設定します。

デフォルト

デフォルトの間隔はそれぞれ 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、バッファ割り当て間隔を 200 秒、コード スペースのチェックサムの間隔を 500 秒に設定する例を示します。

```
hostname(config)# checkheaps check-interval 200
```

```
hostname(config)# checkheaps validate-checksum 500
```

関連コマンド

コマンド	説明
show checkheaps	checkheaps 統計情報を表示します。

check-retransmission

TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

check-retransmission

no check-retransmission

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。矛盾する再送信をエンド システムが解釈する際に生じる TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。

セキュリティ アプライアンスは、再送信のデータが元のデータと同じかどうかを確認しようとします。データが一致しない場合、接続がセキュリティ アプライアンスによってドロップされます。この機能がイネーブルの場合、TCP 接続上のパケットは順序どおりにのみ許可されます。詳細については、**queue-limit** コマンドを参照してください。

例

次に、すべての TCP フローで TCP チェック再送信機能をイネーブルにする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
```

```
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

checksum-verification

TCP チェックサムの検証をイネーブルまたはディセーブルにするには、tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

checksum-verification

no checksum-verification

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

チェックサムの検証は、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用して、TCP チェックサムの検証をイネーブルにします。このチェックに失敗すると、パケットはドロップされます。

例

次に、10.0.0.0 ～ 20.0.0.0 の TCP 接続で TCP チェックサムの検証をイネーブルにする例を示します。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap

hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

cipc security-mode authenticated

Cisco IP Communicator（CIPC）Softphone を音声 VLAN シナリオまたはデータ VLAN シナリオに導入する場合に、強制的に CIPC Softphone を認証済みモードで動作させるには、電話プロキシ コンフィギュレーション モードで **cipc security-mode authenticated** コマンドを使用します。

CIPC Softphone が暗号化をサポートしている場合に、このコマンドをオフにするには、このコマンドの **no** 形式を使用します。

cipc security-mode authenticated

no cipc security-mode authenticated

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、このコマンドは、no 形式によってディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

データ VLAN に影響を及ぼそうとするセキュリティ上の脅威から音声ストリームを守るために、複数の VLAN を使用して音声とデータのトラフィックを分離することがセキュリティ上のベスト プラクティスです。ただし、Cisco IP Communicator（CIPC）Softphone アプリケーションは、それぞれの IP Phone に接続する必要があります。IP Phone は、音声 VLAN に常駐しています。この要件により、音声 VLAN とデータ VLAN を分離することが問題になります。これは、SIP プロトコルおよび SCCP プロトコルが広範囲のポートで RTP ポートおよび RTCP ポートをダイナミックにネゴシエートするためです。このダイナミック ネゴシエーションでは、特定の範囲のポートを 2 つの VLAN の間で開く必要があります。

（注） 認証済みモードをサポートしていない旧バージョンの CIPC は、電話プロキシではサポートされていません。

データ VLAN と音声 VLAN の間でのアクセスを広範囲のポートで行わずに、データ VLAN 上の CIPC Softphone を音声 VLAN 上の該当する IP Phone と接続するには、**cipc security-mode authenticated** コマンドを使用して電話プロキシを設定します。

このコマンドを使用すると、電話プロキシが CIPC コンフィギュレーション ファイルを参照し、CIPC Softphone が強制的に（暗号化済みモードではなく）認証済みモードになります。これは、現在のバージョンの CIPC が暗号化済みモードをサポートしていないためです。

このコマンドがイネーブルの場合、電話プロキシは、電話コンフィギュレーション ファイルを解析し、電話が CIPC Softphone かどうかを判別し、セキュリティ モードを認証済みに変更します。またデフォルトでは、電話プロキシがすべての電話を強制的に暗号化済みモードにしている間だけ、CIPC Softphone は認証済みモードをサポートします。

例

次に、**cipc security-mode authenticated** コマンドを使用して、音声 VLAN シナリオまたはデータ VLAN シナリオに Cisco IP Communicator（CIPC）Softphone を導入するときに CIPC Softphone を強制的に認証済みモードで動作させる例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)#cipc security-mode authenticated
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

class（グローバル）

セキュリティ コンテキストの割り当て先のリソース クラスを作成するには、グローバル コンフィギュレーション モードで **class** コマンドを使用します。クラスを削除するには、このコマンドの **no** 形式を使用します。

class *name*

no class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスに関する制限を設定するには、**default** という名前を入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストがセキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

クラスを作成すると、セキュリティ アプライアンスは、クラスに割り当てられる各コンテキストに対してリソースの一部を確保しなくなります。その代わりに、セキュリティ アプライアンスは、コンテキストの上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。クラス用のリソースを設定するには、**limit-resource** コマンドを参照してください。

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限

を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。逆に、すべてのリソースに対する制限を設定してクラスを作成した場合、そのクラスはデフォルト クラスの設定を使用しません。

デフォルトでは、デフォルト クラスは、すべてのコンテキストにリソースへのアクセスを無制限に提供します。ただし、次の制限が適用されます（この制限は、デフォルトではコンテキストあたりの最大許容値が設定されます）。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

class（ポリシー マップ）

クラス マップ トラフィックにアクションを割り当てることができるポリシー マップにクラス マップを割り当てるには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。ポリシー マップからクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class *classmap_name*

no class *classmap_name*

構文の説明

classmap_name	クラス マップの名前を指定します。レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）の場合、レイヤ 3/4 クラス マップ名（**class-map** コマンドまたは **class-map type management** コマンド）を指定する必要があります。インスペクション ポリシー マップ（**policy-map type inspect** コマンド）の場合、インスペクション クラス マップ名（**class-map type inspect** コマンド）を指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用するには、Modular Policy Framework を使用します。レイヤ 3/4 ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map**：アクションを実行するトラフィックを識別します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インスペクション ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map type inspect**：アクションを実行するトラフィックを指定します。

2. **policy-map type inspect**：各クラス マップに関連付けられているアクションを指定します。
   a. **class**：アクションを実行するインスペクション クラス マップを指定します。
   b. *アプリケーション タイプのコマンド*: 各アプリケーション タイプで使用可能なコマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。インスペクション ポリシー マップのクラス コンフィギュレーション モードでサポートされているアクションには、次のものが含まれます。
   - パケットのドロップ
   - 接続のドロップ
   - 接続のリセット
   - ロギング
   - メッセージのレートの制限
   - コンテンツのマスキング

   c. **parameters**：インスペクション エンジンに影響を及ぼすパラメータを設定します。CLI はパラメータ コンフィギュレーション モードに移行します。使用可能なコマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **class-map**：アクションを実行するトラフィックを識別します。
4. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するレイヤ 3/4 クラス マップを指定します。
   b. **inspect** *application inspect_policy_map*：アプリケーション インスペクションをイネーブルにし、特別なアクションを実行するインスペクション ポリシー マップを呼び出します。
5. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

このコンフィギュレーションには、すべてのトラフィックと一致する、**class-default** と呼ばれるクラス マップが必ず含まれています。各レイヤ 3/4 ポリシー マップの末尾には、アクションが定義されていない **class-default** クラス マップがコンフィギュレーションに含まれています。すべてのトラフィックと照合するが、別のクラス マップを作成しない場合、このクラス マップをオプションで使用できます。実際、一部の機能は、**class-default** クラス マップ用にのみ設定できます（**shape** コマンドなど）。

class-default クラス マップを含めて、最大 63 個の **class** コマンドおよび **match** コマンドをポリシー マップに設定できます。

例

次に、**class** コマンドを含む、接続ポリシーの **policy-map** コマンドの例を示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80
```

```
hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、セキュリティ アプライアンスはこの照合を行いません。

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
class-map type management	管理トラフィック用のレイヤ 3/4 クラス マップを作成します。
clear configure policy-map	service-policy コマンドで使用中のポリシー マップを除く、すべてのポリシー マップ コンフィギュレーションを削除します。
match	トラフィック照合パラメータを定義します。
policy-map	ポリシー（それぞれが 1 つ以上のアクションを持つ 1 つ以上のトラフィック クラスの関連付け）を設定します。

class-map

モジュラ ポリシー フレームワークを使用するとき、グローバル コンフィギュレーション モードで **class-map** コマンド（**type** キーワードは指定しない）を使用して、アクションを適用するレイヤ 3 またはレイヤ 4 のトラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map *class_map_name*

no class-map *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このタイプのクラス マップは、レイヤ 3/4 通過トラフィック専用です。セキュリティ アプライアンス宛ての管理トラフィックについては、**class-map type management** コマンドを参照してください。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。1 つのレイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

デフォルトのクラス マップ

コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用するデフォルトのレイヤ 3/4 クラス マップが含まれます。これは、**inspection_default** と呼ばれ、デフォルト インスペクション トラフィックと一致します。

```
class-map inspection_default
 match default-inspection-traffic
```

デフォルトのコンフィギュレーションに存在する別のクラス マップは、class-default と呼ばれ、これはすべてのトラフィックと一致します。

```
class-map class-default
 match any
```

このクラス マップは、すべてのレイヤ 3/4 ポリシー マップの最後に表示され、原則的に、他のすべてのトラフィックでどんなアクションも実行しないようにセキュリティ アプライアンスに通知します。独自の **match any** クラス マップを作成するのではなく、必要に応じて class-default クラス マップを使用できます。実際のところ、class-default で使用可能な機能は、QoS トラフィック シェーピングなどの一部の機能だけです。

最大クラス マップ

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。

設定の概要

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。レイヤ 3/4 クラス マップには、クラス マップに含まれているトラフィックを指定する、**match** コマンド（**match tunnel-group** コマンドおよび **match default-inspection-traffic** コマンドを除く）が 1 つだけ含まれています。

例

次に、4 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp
```

```
hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map type management	セキュリティ アプライアンスへのトラフィック用のクラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type inspect

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type inspect** コマンドを使用して検査アプリケーションに固有の基準と一致を確認します。インスペクション クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type inspect *application* [**match-all** | **match-any**] *class_map_name*

no class-map [**type inspect** *application* [**match-all** | **match-any**]] *class_map_name*

構文の説明

application	照合するアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **sip**
class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-all	（任意）トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。オプションを指定しない場合、**match-all** がデフォルトです。
match-any	（任意）トラフィックがクラス マップと一致するには、1 つ以上の基準と一致する必要があることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	**match-any** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、インスペクション クラス マップを作成して、対象とするトラフィックを指定できます。このクラス マップには、1 つ以上の **match** コマンドが含まれます （あるいは、単一の基準とアクションをペアにする場合は、インスペクション ポリシー マップで **match** コマンドを直接使用できます）。アプリケーション固有の基準を照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラス マップは、複数のトラフィック照合をグループ化します（match-all クラス マップ）。あるいはクラス マップで、照合リストのいずれかを照合できます（match-any クラス マップ）。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラス マップを使用して複数の match コマンドをグループ化できる点と、クラス マップを再使用できる点です。このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップで、接続のドロップ、リセット、またはロギングなどのアクションを指定できます。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次の例では、すべての基準に一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

次の例では、基準のいずれかに一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。

コマンド	説明
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type management

モジュラ ポリシー フレームワーク を使用するとき、グローバル コンフィギュレーション モードで **class-map type management** コマンドを使用して、アクションを適用するセキュリティ アプライアンス宛ての、レイヤ 3 またはレイヤ 4 の管理トラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type management *class_map_name*

no class-map type management *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	セキュリティ アプライアンスに向かう管理トラフィックの場合、レイヤ 3/4 管理クラス マップに **set connection** コマンドが使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。

使用上のガイドライン

このタイプのクラス マップは、管理トラフィック専用です。通過トラフィックについては、**class-map** コマンド（**type** キーワードは指定しない）を参照してください。

セキュリティ アプライアンスへの管理トラフィックに対して、この種類のトラフィックに特有のアクションの実行が必要になる場合があります。ポリシー マップの管理クラス マップで設定可能なアクションのタイプは、管理トラフィック専用です。たとえば、このタイプのクラス マップでは、RADIUS アカウンティング トラフィックをインスペクトして、接続制限を設定できます。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。

レイヤ 3/4 ポリシー マップそれぞれに、複数のレイヤ 3/4 クラス マップ（管理トラフィックまたは通過トラフィック）を作成できます。

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドおよび **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを識別します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map type management コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。管理クラス マップを指定して、アクセス リストまたは TCP や UDP のポートと照合できます。レイヤ 3/4 クラス マップには、クラス マップに含まれるトラフィックを指定する **match** コマンドが 1 つだけが含まれています。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、レイヤ 3/4 管理クラス マップを作成する例を示します。

```
hostname(config)# class-map type management radius_acct
hostname(config-cmap)# match port tcp eq 10000
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type regex

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type regex** コマンドを使用して、一致テキストで利用する正規表現をグループ化します。正規表現クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-any	トラフィックが正規表現のいずれかとだけ一致する場合でも、このトラフィックがクラス マップと一致しているとすることを指定します。**match-any** が唯一のオプションです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラス マップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現クラス マップで正規表現をグループ化できます。

正規表現クラス マップを作成する前に、**regex** コマンドを使用して、正規表現を作成します。次に、**match regex** コマンドを使用して、クラス マップ コンフィギュレーション モードで名前を付けられた正規表現を指定します。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、2 つの正規表現を作成し、これを正規表現クラス マップに追加する例を示します。トラフィックに「example.com」または「example2.com」というストリングが含まれている場合、このトラフィックはクラス マップと一致しています。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックと照合するインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
regex	正規表現を作成します。

clear aaa local user fail-attempts

ユーザのロック アウト ステータスを変更しないで、ユーザ認証失敗試行回数を 0 にリセットするには、特権 EXEC モードで **clear aaa local user fail-attempts** コマンドを使用します。

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

構文の説明

all	すべてのユーザについて、失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタを 0 にリセットする特定のユーザ名を指定します。
username	続くパラメータが、失敗試行カウンタを 0 にリセットするユーザのユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザが認証試行を何回か失敗した後に、ユーザ認証を失敗にするには、このコマンドを使用します。

設定された認証試行の失敗数に達すると、ユーザは、システムからロック アウトされ、システム管理者がこのユーザ名のロックを解除するか、またはシステムをリブートするまで、正常にログインできません。ユーザが正常に認証されるか、またはセキュリティ アプライアンスをリブートすると、失敗試行数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。また、コンフィギュレーションが変更されると、システムがカウンタを 0 にリセットします。

ユーザ名のロックまたはアンロックにより、システム ログ メッセージが生成されます。特権レベル 15 のシステム管理者は、ロック アウトされません。

例

次に、**clear aaa local user authentication fail-attempts** コマンドを使用して、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

次に、**clear aaa local user authentication fail-attempts** コマンドを使用して、すべてのユーザの失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts all
```

```
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザ認証試行の回数制限を設定します。
clear aaa local user lockout	ユーザのロックアウト ステータスを変更することなく、失敗ユーザ認証試行の回数をゼロにリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa local user lockout

指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定するには、特権 EXEC モードで **clear aaa local user lockout** コマンドを使用します。

clear aaa local user lockout {**username** *name* | **all**}

構文の説明

all	すべてのユーザについて、失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタを 0 にリセットする特定のユーザ名を指定します。
username	続くパラメータが、失敗試行カウンタを 0 にリセットするユーザのユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

username オプションを使用して単一のユーザを指定するか、**all** オプションを使用してすべてのユーザを指定できます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響します。

管理者をデバイスからロックアウトすることはできません。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

例

次に、**clear aaa local user lockout** コマンドを使用して、ユーザ名 anyuser のロックアウト状態をクリアし、失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザ認証試行の回数制限を設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更することなく、失敗ユーザ認証試行の回数をゼロにリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa-server statistics

AAA サーバの統計情報をリセットするには、特権 EXEC モードで **clear aaa-server statistics** コマンドを使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

LOCAL	（任意）LOCAL ユーザ データベースの統計情報をクリアします。
groupname	（任意）グループ内のサーバの統計情報をクリアします。
host *hostname*	（任意）グループ内の特定のサーバの統計情報をクリアします。
protocol *protocol*	（任意）次に指定するプロトコルのサーバの統計情報をクリアします。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

すべてのグループのすべての AAA サーバの統計情報を削除します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコルの値において、以前の **nt-domain** から **nt** に、以前の **rsa-ace** から **sdi** に置き換えられました。

例

次に、グループ内の特定のサーバの AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次に、サーバ グループ全体の AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics svrgrp1
```

次に、すべてのサーバ グループの AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics
```

次に、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ接続データのグループ化の指定および管理を行います。
clear configure aaa-server	デフォルト以外のすべての AAA サーバ グループを削除するか、または指定したグループをクリアします。
show aaa-server	AAA サーバの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバ コンフィギュレーションの値を表示します。

clear access-list

アクセス リスト カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear access-list** コマンドを使用します。

clear access-list *id* **counters**

構文の説明

counters	アクセス リストのカウンタをクリアします。
id	アクセス リストの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear access-list コマンドを入力したら、カウンタをクリアするアクセスリストの *ID* を指定します。そうしないと、カウンタはクリアされません。

例

次に、特定のアクセス リスト カウンタをクリアする例を示します。

```
hostname# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	OSPF ルートの宛先 IP アドレスを識別するアクセス リストを追加します。このアクセス リストは、OSPF 再配布のルート マップで使用できます。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	セキュリティ アプライアンスで実行中のアクセス リスト コンフィギュレーションを表示します。

clear arp

ダイナミック ARP エントリまたは ARP 統計情報をクリアするには、特権 EXEC モードで **clear arp** コマンドを使用します。

clear arp [**statistics**]

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、すべての ARP 統計情報をクリアする例を示します。

```
hostname# clear arp statistics
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear asp drop

高速セキュリティ パスのドロップ統計情報をクリアするには、特権 EXEC モードで **clear asp drop** コマンドを使用します。

clear asp drop [**flow** *type* | **frame** *type*]

構文の説明

flow	（任意）ドロップされたフロー統計情報をクリアします。
frame	（任意）ドロップされたパケット統計情報をクリアします。
type	（任意）特定のプロセスのためにドロップされたフロー統計情報またはパケット統計情報をクリアします。タイプのリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトでは、このコマンドを使用すると、すべてのドロップ統計情報がクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プロセス タイプには、次のものが含まれます。

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

例

次に、すべてのドロップ統計情報をクリアする例を示します。

```
hostname# clear asp drop
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

clear asp table

asp arp テーブルまたは asp classify テーブルのいずれか、あるいはこの両方でヒット カウンタをクリアするには、特権 EXEC モードで **clear asp table** コマンドを使用します。

clear asp table [**arp** | **classify**]

構文の説明

arp	asp arp テーブルのみでヒット カウンタをクリアします。
classify	asp classify テーブルのみでヒット カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

clear asp table コマンドでヒットを指定するオプションは arp と classify の 2 つだけです。

例

次に、すべてのドロップ統計情報をクリアする例を示します。

```
hostname# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

関連コマンド

コマンド	説明
show asp table arp	高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。

clear blocks

最低水準点や履歴情報などのパケット バッファ カウンタをリセットするには、特権 EXEC モードで **clear blocks** コマンドを使用します。

clear blocks

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、このコマンドは、前回のバッファ割り当ての失敗時に保存された履歴情報をクリアします。

例

次に、ブロックをクリアする例を示します。

```
hostname# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てるメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear-button

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される WebVPN ページ ログイン フィールドの [Clear] ボタンをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **clear-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのテキストは「Clear」です。

デフォルトのスタイルは、border:1px solid black;background-color:white;font-weight:bold;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Clear] ボタンのデフォルトの背景色を黒から青に変更する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# clear-button style background-color:blue
```

関連コマンド

コマンド	説明
login-button	WebVPN ページの Login フィールドのログイン ボタンをカスタマイズします。
login-title	WebVPN ページの Login フィールドのタイトルをカスタマイズします。
group-prompt	WebVPN ページの Login フィールドのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページの Login フィールドのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページの Login フィールドのユーザ名プロンプトをカスタマイズします。

clear capture

キャプチャ バッファをクリアするには、特権 EXEC コンフィギュレーション モードで **clear capture** *capture_name* コマンドを使用します。

clear capture *capture_name*

構文の説明

capture_name	パケット キャプチャの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

誤ってすべてのパケット キャプチャを破棄することを防止するために、**clear capture** の短縮形（たとえば、**cl cap** や **clear cap**）は、サポートされていません。

例

次に、キャプチャ バッファ「example」のキャプチャ バッファをクリアする例を示します。

```
hostname(config)# clear capture example
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

clear compression

すべての SVC および WebVPN の接続の圧縮統計情報をクリアするには、特権 EXEC モードで **clear compression** コマンドを使用します。

clear compression {**all** | **svc** | **http-comp**}

構文の説明

all	すべての圧縮統計情報をクリアします。
http-comp	HTTP-COMP 統計情報をクリアします。
svc	SVC 圧縮統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、ユーザの圧縮コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して、SVC 接続経由でのデータの圧縮をイネーブルにします。

CHAPTER 6

clear configure コマンド～ clear configure zonelabs-integrity コマンド

clear configure

実行コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure** コマンドを使用します。

clear configure {**primary** | **secondary** | **all** | *command*}

構文の説明

all	実行コンフィギュレーション全体をクリアします。
command	指定したコマンドのコンフィギュレーションをクリアします。詳細については、このマニュアルの各 **clear configure** *command* コマンドの個々のエントリを参照してください。
primary	次のコマンドを含む、接続に関連するコマンドをクリアします。 • **tftp-server** • **shun** • **route** • **ip address** • **mtu** • **failover** • **monitor-interface** • **boot**
secondary	**primary** キーワードを使用してクリアされる接続に関連しないコマンドをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドをセキュリティ コンテキストで入力すると、コンテキスト コンフィギュレーションだけがクリアされます。このコマンドをシステム実行スペースで入力すると、システム実行コンフィギュレーションと、すべてのコンテキスト実行コンフィギュレーションがクリアされます。システム コンフィギュレーション内のすべてのコンテキスト エントリがクリアされるため（**context** コマンドを参照）、コンテキストは実行されなくなり、コンテキスト実行スペースに移動できなくなります。

コンフィギュレーションをクリアする前に、（スタートアップ コンフィギュレーションの場所を指定する）**boot config** コマンドへのすべての変更をスタートアップ コンフィギュレーションに必ず保存してください。スタートアップ コンフィギュレーションの場所を実行コンフィギュレーション内だけで変更した場合、再起動時にコンフィギュレーションはデフォルトの場所からロードされます。

例

次に、実行コンフィギュレーション全体をクリアする例を示します。

```
hostname(config)# clear configure all
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力されたコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

clear configure aaa

aaa コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure aaa** コマンドを使用します。**clear configure aaa** コマンドは、コンフィギュレーションから AAA コマンド ステートメントを削除します。

clear configure aaa

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、CLI 内での一貫性のために修正されました。

使用上のガイドライン

また、このコマンドは、AAA パラメータ（存在する場合）をデフォルト値にリセットします。

取り消し操作はありません。

例

```
hostname(config)# clear configure aaa
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがアクセスしたネットワーク サービスに関するレコードの保持をイネーブル化、ディセーブル化、または表示します。
aaa authentication	**aaa-server** コマンドで指定したサーバ上での LOCAL、TACACS+、または RADIUS のユーザ認証、あるいは ASDM ユーザ認証をイネーブル化または表示します。
aaa authorization	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
show running-config aaa	AAA コンフィギュレーションを表示します。

clear configure aaa-server

すべての AAA サーバ グループを削除するには、または指定したグループをクリアするには、グローバル コンフィギュレーション モードで **clear configure aaa-server** コマンドを使用します。

clear configure aaa-server [*server-tag*]

clear configure aaa-server [*server-tag*] **host** *server-ip*

構文の説明

server-ip	AAA サーバの IP アドレス。
server-tag	（任意）クリアするサーバ グループの記号名。

デフォルト

すべての AAA サーバ グループを削除します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

特定の AAA サーバ グループ、またはデフォルトで、すべての AAA サーバ グループを指定できます。

サーバ グループ内の特定のサーバを指定するには、**host** キーワードを使用します。

また、このコマンドは、AAA サーバ パラメータ（存在する場合）をデフォルト値にリセットします。

例

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# sdi-version sdi-5
hostname(config-aaa-server)# exit
```

上記のコンフィギュレーションを前提として、次のコマンドは、グループから特定のサーバを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1 host 1.2.3.4
```

次のコマンドは、1 つのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1
```

次のコマンドは、すべてのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ接続データを指定および管理します。
aaa-server protocol	すべてのホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定できます。
show running-config aaa	他の AAA コンフィギュレーション値とともに、ユーザ 1 人あたりに許可する同時プロキシ接続の現在の最大数を表示します。

clear configure access-group

すべてのインターフェイスからアクセス グループを削除するには、グローバル コンフィギュレーション モードで **clear configure access-group** コマンドを使用します。

clear configure access-group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

例

次に、すべてのアクセス グループを削除する例を示します。

```
hostname(config)# clear configure access-group
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
show running-config access-group	現在のアクセス グループ コンフィギュレーションを表示します。

clear configure access-list

実行コンフィギュレーションからアクセス リストをクリアするには、グローバル コンフィギュレーション モードで **clear configure access list** コマンドを使用します。

clear configure access-list [*id*]

構文の説明

id	（任意）アクセス リストの名前または番号。

デフォルト

実行コンフィギュレーションからすべてのアクセス リストがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear configure access-list コマンドは、**crypto map** コマンドまたはインターフェイスからアクセス リストを自動的にアンバインドします。**crypto map** コマンドからアクセス リストをアンバインドすると、すべてのパケットが廃棄される状態になる場合があります。これは、アクセス リストを参照している **crypto map** コマンドが不完全なものになるためです。この状態を解消するには、他の **access-list** コマンドを定義して **crypto map** コマンドを完全なものにするか、**access-list** コマンドに関係する **crypto map** コマンドを削除します。詳細については、**crypto map client** コマンドを参照してください。

例

次に、実行コンフィギュレーションからアクセス リストをクリアする例を示します。

```
hostname(config)# clear configure access-list
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	OSPF ルートの宛先 IP アドレスを識別するアクセス リストを追加します。このアクセス リストは、OSPF 再配布のルート マップで使用できます。
clear access-list	アクセス リストのカウンタをクリアします。

コマンド	説明
show access-list	アクセス リストのカウンタを表示します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

clear configure alias

コンフィギュレーションからすべての **alias** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure alias** コマンドを使用します。

clear configure alias

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、コンフィギュレーションからすべての **alias** コマンドを削除する例を示します。

```
hostname(config)# clear configure alias
```

関連コマンド

コマンド	説明
alias	あるアドレスを別のアドレスに変換します。
show running-config alias	コンフィギュレーション内のデュアル NAT コマンドと重複しているアドレスを表示します。

clear configure arp

arp コマンドで追加したスタティック ARP エントリをクリアするには、グローバル コンフィギュレーション モードで **clear configure arp** コマンドを使用します。

clear configure arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、コンフィギュレーションからスタティック ARP エントリをクリアする例を示します。

```
hostname(config)# clear configure arp
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure arp-inspection

ARP インスペクションのコンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure arp-inspection** コマンドを使用します。

clear configure arp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ARP インスペクションのコンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure arp-inspection
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure asdm

実行コンフィギュレーションからすべての **asdm** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure asdm** コマンドを使用します。

clear configure asdm [**location** | **group** | **image**]

構文の説明

group	（任意）実行コンフィギュレーションから **asdm group** コマンドだけをクリアします。
image	（任意）実行コンフィギュレーションから **asdm image** コマンドだけをクリアします。
location	（任意）実行コンフィギュレーションから **asdm location** コマンドだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear pdm** コマンドから **clear configure asdm** コマンドに変更されました。

使用上のガイドライン

実行コンフィギュレーション内の **asdm** コマンドを表示するには、**show running-config asdm** コマンドを使用します。

コンフィギュレーションから **asdm image** コマンドをクリアすると、ASDM アクセスがディセーブルになります。コンフィギュレーションから **asdm location** コマンドと **asdm group** コマンドをクリアすると、ASDM は、次回アクセスされたときにこれらのコマンドを再生成しますが、アクティブな ASDM セッションが妨げられる場合があります。

（注） マルチ コンテキスト モードで実行されているセキュリティ アプライアンスでは、**clear configure asdm image** コマンドはシステム実行スペースでのみ使用できます。一方、**clear configure asdm group** コマンドおよび **clear configure asdm location** コマンドは、ユーザ コンテキストでのみ使用できます。

例

次に、実行コンフィギュレーションから **asdm group** コマンドをクリアする例を示します。

```
hostname(config)# clear configure asdm group
hostname(config)#
```

関連コマンド

コマンド	説明
asdm group	オブジェクト グループ名をインターフェイスに関連付けるために、ASDM によって使用されます。
asdm image	ASDM イメージ ファイルを指定します。
asdm location	IP アドレスをインターフェイス アソシエーションに記録するために、ASDM によって使用されます。
show running-config asdm	実行コンフィギュレーション内の **asdm** コマンドを表示します。

clear configure auth-prompt

前に指定した認証プロンプト チャレンジ テキストを削除し、デフォルト値（存在する場合）に戻すには、グローバル コンフィギュレーション モードで **clear configure auth-prompt** コマンドを使用します。

clear configure auth-prompt

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI 規格に適合するようにこのコマンドが変更されました。

使用上のガイドライン

認証プロンプトをクリアした後、ユーザのログイン時に表示されるプロンプトは、使用するプロトコルによって次のように異なります。

- HTTP を使用してログインするユーザの場合、`HTTP Authentication` が表示されます。
- FTP を使用してログインするユーザの場合、`FTP Authentication` が表示されます。
- Telnet を使用してログインするユーザの場合、プロンプトは表示されません。

例

次に、認証プロンプトをクリアする例を示します。

```
hostname(config)# clear configure auth-prompt
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
show running-config auth-prompt	ユーザ認可プロンプトを表示します。

clear configure banner

すべてのバナーを削除するには、グローバル コンフィギュレーション モードで **clear configure banner** コマンドを使用します。

clear configure banner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、バナーをクリアする例を示します。

```
hostname(config)# clear configure banner
```

関連コマンド

コマンド	説明
banner	セッション バナー、ログイン バナー、または Message-of-The-Day バナーを設定します。
show running-config banner	すべてのバナーを表示します。

clear configure ca certificate map

すべての証明書マップ エントリ、または指定した証明書マップ エントリを削除するには、グローバル コンフィギュレーション モードで **clear configure ca configurate map** コマンドを使用します。

clear configure ca certificate map [*sequence-number*]

構文の説明

sequence-number	（任意）削除する証明書マップ ルールの番号を指定します。指定できる範囲は 1 ～ 65535 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべての証明書マップ エントリを削除する例を示します。

```
hostname(config)# clear configure ca certificate map
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。

clear configure class

リソース クラス コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure class** コマンドを使用します。

clear configure class

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、クラス コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure class
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

clear configure class-map

すべてのクラス マップを削除するには、グローバル コンフィギュレーション モードで **clear configure class-map** コマンドを使用します。

clear configure class-map [**type** {**management** | **regex** | **inspect** [*protocol*]}

構文の説明

inspect	（任意）インスペクション クラス マップをクリアします。
management	（任意）管理クラス マップをクリアします。
protocol	（任意）クリアするアプリケーション マップのタイプを指定します。利用可能なタイプは次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	（任意）正規表現クラス マップをクリアします。
type	（任意）クリアするクラス マップのタイプを指定します。レイヤ 3/4 クラス マップをクリアする場合は、タイプを指定しません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定の名前のクラス マップをクリアするには、**class-map** コマンドの **no** 形式を使用します。

例

次に、設定済みのすべてのクラス マップをクリアする例を示します。

```
hostname(config)# clear configure class-map
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

clear configure client-update

クライアント更新を強制する機能をコンフィギュレーションから削除するには、グローバル コンフィギュレーション モードまたはトンネル グループ ipsec 属性コンフィギュレーション モードで **clear configure client-update** コマンドを使用します。

clear configure client-update

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。

例

次に、グローバル コンフィギュレーション モードで、コンフィギュレーションからクライアント更新機能を削除する例を示します。

```
hostname(config)# clear configure client-update
hostname(config)#
```

次に、トンネル グループ ipsec 属性コンフィギュレーション モードで、test という名前のトンネル グループのコンフィギュレーションからクライアント更新機能を削除する例を示します。

```
hostname(config)# tunnel-group test ipsec-attributes
hostname(config-tunnel-ipsec)# clear configure client-update
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
client-update	クライアント アップデートを設定します。
show running-config client-update	現在のクライアント アップデート コンフィギュレーションを表示します。

clear configure clock

クロック コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure clock** コマンドを使用します。

clear configure clock

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear clock** から変更されました。

使用上のガイドライン

このコマンドは、すべての **clock** コンフィギュレーション コマンドをクリアします。**clock set** コマンドはコンフィギュレーション コマンドではないため、このコマンドはクロックをリセットしません。クロックをリセットするには、**clock set** コマンドの新しい時刻を設定する必要があります。

例

次に、すべての clock コマンドをクリアする例を示します。

```
hostname# clear configure clock
```

関連コマンド

コマンド	説明
clock set	時間を手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。

clear configure command-alias

デフォルト以外のコマンド エイリアスをすべて削除するには、グローバル コンフィギュレーション モードで **clear configure command-alias** コマンドを使用します。

clear configure command-alias

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、デフォルト以外のコマンド エイリアスをすべて削除する例を示します。

```
hostname(config)# clear configure command-alias
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
show running-config command-alias	デフォルト以外のコマンド エイリアスをすべて表示します。

clear configure compression

グローバル圧縮コンフィギュレーションをデフォルト（すべての圧縮技術がイネーブル）にリセットするには、グローバル コンフィギュレーション モードで **clear configure compression** コマンドを使用します。

clear configure compression

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、圧縮コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、およびポート転送接続に対して圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して SVC 接続を介する HTTP データの圧縮をイネーブルにします。

clear configure console

コンソール接続設定をデフォルトにリセットするには、グローバル コンフィギュレーション モードで **clear configure console** コマンドを使用します。

clear configure console

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、コンソール接続設定をデフォルトにリセットする例を示します。

```
hostname(config)# clear configure console
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

clear configure context

システム コンフィギュレーション内のすべてのコンテキスト コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure context** コマンドを使用します。

clear configure context [**noconfirm**]

構文の説明

noconfirm	（任意）確認を求めるプロンプトを表示せずにすべてのコンテキストを削除します。このオプションは自動スクリプトで役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、管理コンテキストを含むすべてのコンテキストを削除できます。管理コンテキストは、**no context** コマンドを使用して削除することはできませんが、**clear configure context** コマンドを使用して削除できます。

例

次に、システム コンフィギュレーションからすべてのコンテキストを削除し、削除を確認しない例を示します。

```
hostname(config)# clear configure context noconfirm
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

コマンド	説明
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

clear configure crypto

IPSec、クリプト マップ、ダイナミック クリプト マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、および ISAKMP を含む、クリプト コンフィギュレーション全体を削除するには、グローバル コンフィギュレーションで **clear configure crypto** コマンドを使用します。特定のコンフィギュレーションを削除するには、構文に示されているように、このコマンドをキーワードとともに使用します。このコマンドは注意して使用してください。

clear configure crypto [**ca** | **dynamic-map** | **ipsec** | **iskmp** | **map**]

構文の説明

ca	認証局のポリシーを削除します。
dynamic-map	ダイナミック クリプト マップ コンフィギュレーションを削除します。
ipsec	IPSec コンフィギュレーションを削除します。
isakmp	ISAKMP コンフィギュレーションを削除します。
map	クリプト マップ コンフィギュレーションを削除します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで発行され、セキュリティ アプライアンスからすべてのクリプト コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure crypto
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	コンフィギュレーションから、すべてのダイナミック クリプト マップまたは指定したダイナミック クリプト マップをクリアします。
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。

コマンド	説明
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show running-config crypto	IPSec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など暗号コンフィギュレーション全体を表示します。

clear configure crypto ca trustpoint

コンフィギュレーションからすべてのトラストポイントを削除するには、グローバル コンフィギュレーションで **clear configure crypto ca trustpoint** コマンドを使用します。

clear configure crypto ca trustpoint

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、コンフィギュレーションからすべてのトラストポイントを削除する例を示します。

```
hostname(config)# clear configure crypto ca trustpoint
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブコンフィギュレーション レベルに入ります。

clear configure crypto dynamic-map

コンフィギュレーションからすべてのダイナミック クリプト マップまたは指定したダイナミック クリプト マップを削除するには、グローバル コンフィギュレーションで **clear configure crypto dynamic-map** コマンドを使用します。

clear configure crypto dynamic-map *dynamic-map-name dynamic-seq-num*

構文の説明

dynamic-map-name	特定のダイナミック クリプト マップの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、コンフィギュレーションからシーケンス番号 3 のダイナミック クリプト マップ mymaps を削除する例を示します。

```
hostname(config)# clear configure crypto dynamic-map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップまたは指定したクリプト マップのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのアクティブなコンフィギュレーションをすべて表示します。
show running-config crypto map	すべてのクリプト マップのアクティブなコンフィギュレーションをすべて表示します。

clear configure crypto isakmp

すべての ISAKMP コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure crypto isakmp** コマンドを使用します。

clear configure crypto isakmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp** コマンドで置換されています。

例

次のコマンドは、グローバル コンフィギュレーション モードで発行され、すべての ISAKMP コンフィギュレーションをセキュリティ アプライアンスから削除しています。

```
hostname(config)# clear configure crypto isakmp
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show crypto isakmp stats	実行時統計情報を表示します。
show crypto isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure crypto isakmp policy

すべての ISAKMP ポリシー コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp policy** コマンドを使用します。

clear configure crypto isakmp policy *priority*

構文の説明

priority	クリアする ISAKMP プライオリティのプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp policy** コマンドが導入されました。
7.2(1)	**clear configure isakmp policy** コマンドが、**clear configure crypto isakmp policy** コマンドに置き換えられました。

例

次に、プライオリティ 3 の ISAKMP ポリシーをコンフィギュレーションから削除する例を示します。

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

関連コマンド

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure crypto map

コンフィギュレーションからすべてのクリプト マップまたは指定したクリプト マップを削除するには、グローバル コンフィギュレーションで **clear configure crypto map** コマンドを使用します。

clear configure crypto map *map-name seq-num*

構文の説明

map-name	特定のクリプト マップの名前を指定します。
seq-num	クリプト マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、コンフィギュレーションからシーケンス番号 3 のクリプト マップ mymaps を削除する例を示します。

```
hostname(config)# clear configure crypto map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプトマップまたは指定したダイナミック クリプト マップのコンフィギュレーションをクリアします。
crypto map interface	クリプト マップをインターフェイスに適用します。
show running-config crypto map	すべてのクリプト マップのアクティブなコンフィギュレーションを表示します。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのアクティブなコンフィギュレーションを表示します。

clear configure ctl-file

設定されている CTL ファイル インスタンスをクリアするには、グローバル コンフィギュレーション モードで **clear configure ctl-file** コマンドを使用します。

clear configure ctl [*ctl_name*]

構文の説明

ctl_name	（任意）CTL インスタンスの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**clear configure ctl-file** コマンドを使用して、設定されている CTL ファイル インスタンスをクリアする例を示します。

```
hostname# clear configure ctl asa_phone_proxy asa_ctl
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（**Phone-Proxy**）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

clear configure ctl-provider

設定されているすべての証明書信頼リスト プロバイダー インスタンスを削除するには、グローバル コンフィギュレーション モードで **clear configure ctl-provider** コマンドを使用します。

clear configure ctl-provider

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**clear configure ctl-provider** コマンドの構文例を示します。

```
hostname# clear configure ctl-provider
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。

clear configure ddns

すべての DDNS コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure ddns** コマンドを使用します。

clear configure ddns

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、すべての DDNS コマンドをクリアする例を示します。

```
hostname(config)# clear configure ddns
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	セキュリティ アプライアンス インターフェイスを DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（**グローバル コンフィギュレーション モード**）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。
show ddns update method	設定済みの DDNS 方式ごとにタイプと間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

clear configure dhcpd

DHCP サーバ コマンド、バインディング、および統計情報をすべてクリアするには、グローバル コンフィギュレーション モードで **clear configure dhcpd** コマンドを使用します。

clear configure dhcpd

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear dhcpd** から **clear configure dhcpd** に変更されました。

使用上のガイドライン

clear configure dhcpd コマンドは、**dhcpd** コマンド、バインディング、および統計情報をすべてクリアします。統計情報カウンタまたはバインディング情報だけをクリアするには、**clear dhcpd** コマンドを使用します。

例

次に、すべての **dhcpd** コマンドをクリアする例を示します。

```
hostname(config)# clear configure dhcpd
```

関連コマンド

コマンド	説明
clear dhcpd	DHCP サーバ バインディングおよび統計情報カウンタをクリアします。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

clear configure dhcprelay

すべての DHCP リレー コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure dhcprelay** コマンドを使用します。

clear configure dhcprelay

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear dhcprelay** から **clear configure dhcprelay** に変更されました。

使用上のガイドライン

clear configure dhcprelay コマンドは、DHCP リレーの統計情報およびコンフィギュレーションをクリアします。DHCP 統計情報カウンタだけをクリアするには、**clear dhcprelay statistics** コマンドを使用します。

例

次に、DHCP リレー コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure dhcprelay
```

関連コマンド

コマンド	説明
clear dhcprelay statistics	DHCP リレー エージェントの統計カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

clear configure dns

すべての DNS コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure dns** コマンドを使用します。

clear configure dns

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべての DNS コマンドをクリアする例を示します。

```
hostname(config)# clear configure dns
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear configure dynamic-access-policy-config

DAP コンフィギュレーションをクリアするには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **clear configure dynamic-access-policy-config** コマンドを使用します。

clear config dynamic-access-policy-config *name*

構文の説明

name	DAP コンフィギュレーション ファイルの名前を指定するストリング。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、Finance という DAP レコードにプライオリティ 15 を設定する例を示します。

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# priority 15
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

clear config dynamic-access-policy-record

DAP レコードをクリアするには、グローバル コンフィギュレーション モードでレコードの名前を指定して **clear config dynamic-access-policy-record** コマンドを使用します。すべての DAP レコードをクリアするには、このコマンドの **no** 形式を使用します。

clear config dynamic-access-policy-record *name*

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、Finance という名前の DAP レコードをクリアする例を示します。

```
hostname(config)# clear configure dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record [*name*]	指定した DAP レコードを作成します。
dynamic-access-policy-config url	DAP 選択コンフィギュレーション ファイルを設定します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

clear configure established

確立されたコマンドをすべて削除するには、グローバル コンフィギュレーション モードで **clear configure established** コマンドを使用します。

clear configure established

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

使用上のガイドライン

established コマンドで作成した確立済みの接続を削除するには、**clear xlate** コマンドを入力します。

例

次に、確立されているコマンドを削除する例を示します。

```
hostname(config)# clear configure established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。
clear xlate	現在の変換および接続スロット情報をクリアします。

clear configure failover

コンフィギュレーションから **failover** コマンドを削除してデフォルトに戻すには、グローバル コンフィギュレーション モードで **clear configure failover** コマンドを使用します。

clear configure failover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear failover** から **clear configure failover** に変更されました。

使用上のガイドライン

このコマンドは、実行コンフィギュレーションからすべての **failover** コマンドをクリアし、デフォルトに戻します。**all** キーワードを **show running-config failover** コマンドで使用すると、デフォルトのフェールオーバー コンフィギュレーションが表示されます。

clear configure failover コマンドは、マルチ コンフィギュレーション モードのセキュリティ コンテキストでは使用できません。このコマンドはシステム実行スペースで入力する必要があります。

例

次に、コンフィギュレーションからすべての failover コマンドをクリアする例を示します。

```
hostname(config)# clear configure failover
hostname(config)# show running-configuration failover
no failover
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

clear configure filter

URL、FTP、および HTTPS フィルタリング コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure filter** コマンドを使用します。

clear configure filter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure filter コマンドは、URL、FTP、および HTTPS フィルタリング コンフィギュレーションをクリアします。

例

次に、URL、FTP、および HTTPS フィルタリング コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure filter
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure fips

NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアするには、グローバル コンフィギュレーション モードで **clear configure fips** コマンドを使用します。

clear configure fips

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

例

```
hostname(config)# clear configure fips
```

関連コマンド

コマンド	説明
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

clear configure firewall

ファイアウォール モードをデフォルトのルーテッド モードに設定するには、グローバル コンフィギュレーション モードで **clear configure firewall** コマンドを使用します。

clear configure firewall

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ファイアウォール モードをデフォルトに設定する例を示します。

```
hostname(config)# clear configure firewall
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure fixup

フィックスアップ コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure fixup** コマンドを使用します。

clear configure fixup

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear configure fixup コマンドは、フィックスアップ コンフィギュレーションを削除します。

例

次に、フィックスアップ コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

clear configure fragment

すべての IP フラグメント再構築コンフィギュレーションをデフォルトにリセットするには、グローバル コンフィギュレーション モードで **clear configure fragment** コマンドを使用します。

clear configure fragment [*interface*]

構文の説明

interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**configure** キーワードおよびオプションの *interface* 引数が追加されました。また、このコマンドは、コンフィギュレーション データのクリアを動作データのクリアと区別するために、**clear fragment** と **clear configure fragment** の 2 つのコマンドに分けられました。

使用上のガイドライン

clear configure fragment コマンドは、すべての IP フラグメント再構築コンフィギュレーションをデフォルト値にリセットします。さらに、**chain**、**size**、および **timeout** の各キーワードが、次に示すそれぞれのデフォルト値にリセットされます。

- **chain** は 24 パケットです。
- **size** は 200 です。
- **timeout** は 5 秒です。

例

次に、すべての IP フラグメント再構築コンフィギュレーションをデフォルト値にリセットする例を示します。

```
hostname(config)# clear configure fragment
```

関連コマンド

コマンド	説明
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。

コマンド	説明
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear configure ftp

FTP コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure ftp** コマンドを使用します。

clear configure ftp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure ftp コマンドは、FTP コンフィギュレーションをクリアします。

例

次に、FTP コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure ftp
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure global

コンフィギュレーションから **global** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure global** コマンドを使用します。

clear configure global

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

例

次に、コンフィギュレーションから **global** コマンドを削除する例を示します。

```
hostname(config)# clear configure global
```

関連コマンド

コマンド	説明
global	グローバル アドレスのプールからエントリを作成します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。

clear configure group-delimiter

トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するグループ デリミタをコンフィギュレーションから削除するには、グローバル コンフィギュレーション モードで **clear configure group-delimiter** コマンドを使用します。グループ名の解析がディセーブルになります。

clear config group-delimiter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デリミタは、トンネルのネゴシエーション中に、ユーザ名からトンネル グループ名を解析するために使用されます。デリミタが指定されていない場合、グループ名の解析はディセーブルになります。

例

次に、グローバル コンフィギュレーション モードで、グループ デリミタをコンフィギュレーションから削除する例を示します。

```
hostname(config)# clear config group-delimiter
hostname(config)#
```

関連コマンド

コマンド	説明
group-delimiter	グループ名の解析をイネーブルにし、IPSec リモート アクセス トンネル グループのグループ デリミタを指定します。
show running-config group-delimiter	現在の設定済みグループ デリミタを表示します。

clear configure group-policy

特定のグループ ポリシーのコンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure group-policy** コマンドを使用し、グループ ポリシーの名前を付加します。すべての group-policy コマンド（デフォルトのグループ ポリシーは除く）をコンフィギュレーションから削除するには、このコマンドを引数なしで使用します。

clear configure group-policy [*name*]

構文の説明

name	（任意）グループ ポリシーの名前を指定します。

デフォルト

すべての group-policy コマンド（デフォルトのグループ ポリシーは除く）をコンフィギュレーションから削除します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーのコンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成、編集、または削除します。
group-policy attributes	グループ ポリシー属性モードを開始します。このモードでは、指定したグループ ポリシーの AVP を設定できます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。

clear configure hostname

ホスト名をデフォルト値にリセットするには、グローバル コンフィギュレーション モードで **clear configure hostname** コマンドを使用します。

clear configure hostname

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はプラットフォームによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ホスト名をクリアする例を示します。

```
hostname(config)# clear configure hostname
```

関連コマンド

コマンド	説明
banner	ログイン バナー、Message-of-The-Day バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。

clear configure http

HTTP サーバをディセーブルにし、HTTP サーバにアクセスできる設定済みホストを削除するには、グローバル コンフィギュレーション モードで **clear configure http** コマンドを使用します。

clear configure http

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、HTTP コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure http
```

関連コマンド

コマンド	説明
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由するセキュリティ アプライアンスのインターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザの証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

clear configure icmp

ICMP トラフィックの設定済みアクセス ルールをクリアするには、グローバル コンフィギュレーション モードで **clear configure icmp** コマンドを使用します。

clear configure icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure icmp コマンドは、ICMP トラフィックの設定済みアクセス ルールをクリアします。

例

次に、ICMP トラフィックの設定済みアクセス ルールをクリアする例を示します。

```
hostname# clear configure icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

clear configure imap4s

コンフィギュレーションからすべての IMAP4S コマンドを削除して、デフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure imap4s** コマンドを使用します。

clear configure imap4s

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IMAP4S コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure imap4s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration imap4s	IMAP4S の実行コンフィギュレーションを表示します。
imap4s	IMAP4S 電子メール プロキシ コンフィギュレーションを作成または編集します。

clear configure interface

インターフェイス コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure interface** コマンドを使用します。

clear configure interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス コンフィギュレーションをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear interface** から変更されました。また、このコマンドは、インターフェイスの新しい番号付け方式を含めるように修正されました。

使用上のガイドライン

メインの物理インターフェイスのインターフェイス コンフィギュレーションをクリアする場合、セキュリティ アプライアンスはデフォルト設定を使用します。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。

例

次に、GigabitEthernet0/1 コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure interface gigabitethernet0/1
```

次に、内部インターフェイス コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure interface inside
```

次に、コンテキスト内で int1 インターフェイス コンフィギュレーションをクリアする例を示します。「int1」はマッピング名です。

```
hostname/contexta(config)# clear configure interface int1
```

次に、すべてのインターフェイス コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure interface
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

clear configure ip

ip address コマンドで設定したすべての IP アドレスをクリアするには、グローバル コンフィギュレーション モードで **clear configure ip** コマンドを使用します。

clear configure ip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トランスペアレント ファイアウォール モードでは、このコマンドは、管理 IP アドレスと Management 0/0 IP アドレス（設定されている場合）をクリアします。

古い IP アドレスを使用している現在の接続をすべて停止するには、**clear xlate** コマンドを入力します。入力しない場合、接続は通常どおりタイムアウトします。

例

次に、すべての IP アドレスをクリアする例を示します。

```
hostname(config)# clear configure ip
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

コマンド	説明
ip address	インターフェイスの IP アドレスを設定します。
show running-config interface	インターフェイスの設定を表示します。

clear configure ip audit

監査ポリシー コンフィギュレーション全体をクリアするには、グローバル コンフィギュレーション モードで **clear configure ip audit** コマンドを使用します。

clear configure ip audit [**configuration**]

構文の説明

configuration	（任意）このキーワードを入力できますが、使用しない場合も結果は同じです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear ip audit** から変更されました。

例

次に、すべての **ip audit** コマンドをクリアする例を示します。

```
hostname# clear configure ip audit
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

clear configure ip local pool

IP アドレス プールを削除するには、グローバル コンフィギュレーション モードで **clear configure ip local pool** コマンドを使用します。

clear ip local pool [*poolname*]

構文の説明

poolname	（任意）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、実行コンフィギュレーションからすべての IP アドレス プールを削除する例を示します。

```
hostname(config)# clear config ip local pool
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

clear configure ip verify reverse-path

ip verify reverse-path コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure ip verify reverse-path** コマンドを使用します。

clear configure ip verify reverse-path

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear ip verify reverse-path** から変更されました。

例

次に、すべてのインターフェイスの **ip verify reverse-path** コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure ip verify reverse-path
```

関連コマンド

コマンド	説明
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear configure ipv6

実行コンフィギュレーションからグローバル IPv6 コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure ipv6** コマンドを使用します。

clear configure ipv6 [**route** | **access-list**]

構文の説明

access-list	（任意）実行コンフィギュレーションから IPv6 アクセス リスト コマンドをクリアします。
route	（任意）実行コンフィギュレーションから、IPv6 ルーティング テーブル内のルートをスタティックに定義するコマンドをクリアします。

デフォルト

キーワードを指定しない場合、このコマンドは、実行コンフィギュレーションからすべての IPv6 コマンドをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、実行コンフィギュレーションからグローバル IPv6 コマンドだけをクリアします。インターフェイス コンフィギュレーション モードで入力した IPv6 コマンドはクリアしません。

例

次に、IPv6 ルーティング テーブルから、スタティックに定義された IPv6 ルートをクリアする例を示します。

```
hostname(config)# clear configure ipv6 route
hostname(config)#
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブル内のスタティック ルートを定義します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show running-config ipv6	実行コンフィギュレーション内の IPv6 コマンドを表示します。

clear configure isakmp

すべての ISAKMP コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp** コマンドを使用します。

clear configure isakmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp** コマンドで置換されています。

例

次に、グローバル コンフィギュレーション モードで発行され、セキュリティ アプライアンスからすべての ISAKMP コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure isakmp
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure isakmp policy

すべての ISAKMP ポリシー コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp policy** コマンドを使用します。

clear configure isakmp policy *priority*

構文の説明

priority	クリアする ISAKMP プライオリティのプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp policy** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp policy** コマンドに置き換えられました。

例

次に、プライオリティ 3 の ISAKMP ポリシーをコンフィギュレーションから削除する例を示します。

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

関連コマンド

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure ldap attribute-map

セキュリティ アプライアンスの実行コンフィギュレーションからすべての LDAP 属性マップを削除するには、グローバル コンフィギュレーション モードで **clear configure ldap attribute-map** コマンドを使用します。

clear configure ldap attribute-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、セキュリティ アプライアンスの実行コンフィギュレーションから LDAP 属性マップを削除します。

例

次に、グローバル コンフィギュレーション モードで、実行コンフィギュレーションからすべての LDAP 属性マップを削除し、**show running-config ldap attribute-map** コマンドを使用して削除を確認する例を示します。

```
hostname(config)# clear configuration ldap attribute-map
hostname(config)# show running-config ldap attribute-map
hostname(config)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。

コマンド	説明
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。

clear configure logging

ロギング コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure logging** コマンドを使用します。

clear configure logging [**disabled** | **level**]

構文の説明

disabled	（任意）ディセーブルになっているすべてのシステム ログ メッセージを再度イネーブルにすることを指定します。このオプションを使用することによって、他にクリアされるロギング コンフィギュレーションはありません。
level	（任意）システム ログ メッセージへの重大度レベルの割り当てをデフォルト値にリセットすることを指定します。このオプションを使用することによって、他にクリアされるロギング コンフィギュレーションはありません。

デフォルト

キーワードを指定しない場合、このコマンドは、すべてのコンフィギュレーション設定をデフォルト値に戻します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config logging コマンドを使用して、すべてのロギング コンフィギュレーション設定を表示できます。**clear configure logging** コマンドを disabled または level キーワードなしで使用した場合、すべてのロギング コンフィギュレーション設定がクリアされ、デフォルト値に戻ります。

例

次に、ロギング コンフィギュレーション設定をクリアする例を示します。**show logging** コマンドの出力は、すべてのロギング機能がディセーブルになっていることを示します。

```
hostname(config)# clear configure logging
hostname(config)# show logging
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

clear configure logging rate-limit

ロギング レート制限をリセットするには、グローバル コンフィギュレーション モードで **clear configure logging rate-limit** コマンドを使用します。

clear configure logging rate-limit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

例

次に、ロギング レート制限をリセットする例を示します。

```
hostname(config)# clear configure logging rate-limit
```

情報がクリアされると、ホストが接続を再確立するまで、何も表示されません。

関連コマンド

コマンド	説明
logging rate limit	システム ログ メッセージが生成されるレートを制限します。
show running config logging rate-limit	現在のロギング レート制限の設定を表示します。

clear configure mac-address-table

mac-address-table static および **mac-address-table aging-time** コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure mac-address-table** コマンドを使用します。

clear configure mac-address-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**mac-address-table static** および **mac-address-table aging-time** コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure mac-address-table
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

clear configure mac-learn

mac-learn コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure mac-learn** コマンドを使用します。

clear configure mac-learn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**mac-learn** コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure mac-learn
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

clear configure mac-list

mac-list コマンドで指定済みの MAC アドレスの指定したリストを削除するには、グローバル コンフィギュレーション モードで **clear configure mac-list** コマンドを使用します。

clear configure mac-list *id*

構文の説明

id	MAC アドレス リスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI 規格に適合するようにこのコマンドが変更されました。

使用上のガイドライン

MAC アドレスのリストを削除するには、**clear mac-list** コマンドを使用します。

例

次に、MAC アドレス リストをクリアする例を示します。

```
hostname(config)# clear configure mac-list firstmaclist
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
show running-config mac-list	*id* 値で指定した MAC アドレス リスト内の MAC アドレスを表示します。

clear configure management-access

セキュリティ アプライアンスの管理アクセス用の内部インターフェイスのコンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure management-access** コマンドを使用します。

clear configure management-access

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドで定義され、**show interface** コマンドの出力で引用符（" "）に囲まれて表示されます）。**clear configure management-access** コマンドは、**management-access** コマンドで指定した内部管理インターフェイスのコンフィギュレーションを削除します。

例

次に、セキュリティ アプライアンスの管理アクセス用の内部インターフェイスのコンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure management-access
```

関連コマンド

コマンド	説明
management-access	管理アクセス用の内部インターフェイスを設定します。
show running-config management-access	管理アクセスのために設定された内部インターフェイスの名前を表示します。

clear configure monitor-interface

実行コンフィギュレーションからすべての **monitor-interface** コマンドを削除し、デフォルトのインターフェイス ヘルス モニタリングに戻すには、グローバル コンフィギュレーション モードで **clear configure monitor-interface** コマンドを使用します。

clear configure monitor-interface

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、物理インターフェイスがフェールオーバーのためにモニタされます。**clear monitor-interface** コマンドを使用すると、実行コンフィギュレーションから **no monitor-interface** コマンドがクリアされ、デフォルトのインターフェイス ヘルス モニタリングに戻ります。実行コンフィギュレーション内の **monitor-interface** コマンドを表示するには、**show running-config all monitor-interface** コマンドを使用します。

例

次に、実行コンフィギュレーションから **monitor-interface** コマンドをクリアする例を示します。

```
hostname(config)# clear configure monitor-interface
hostname(config)#
```

関連コマンド

コマンド	説明
monitor-interface	指定したインターフェイスでフェールオーバーを目的とするヘルス モニタリングをイネーブルにします。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

clear configure mroute

実行コンフィギュレーションから **mroute** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure mroute** コマンドを使用します。

clear configure mroute

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、コンフィギュレーションから **mroute** コマンドを削除する例を示します。

```
hostname(config)# clear configure mroute
hostname(config)#
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	実行コンフィギュレーション内の **mroute** コマンドを表示します。

clear configure mtu

すべてのインターフェイスの設定済み最大伝送単位値をクリアするには、グローバル コンフィギュレーション モードで **clear configure mtu** コマンドを使用します。

clear configure mtu

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

clear configure mtu コマンドを使用すると、すべてのイーサネット インターフェイスの最大伝送単位がデフォルトの 1500 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、すべてのインターフェイスの現在の最大伝送単位値をクリアする例を示します。

```
hostname(config)# clear configure mtu
```

関連コマンド

コマンド	説明
mtu	インターフェイスの最大伝送単位を指定します。
show running-config mtu	現在の最大伝送単位のブロック サイズを表示します。

clear configure multicast-routing

実行コンフィギュレーションから **multicast-routing** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure multicast-routing** コマンドを使用します。

clear configure multicast-routing

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure multicast-routing コマンドは、実行コンフィギュレーションから multicast-routing を削除します。no multicast-routing コマンドも、実行コンフィギュレーションから multicast-routing コマンドを削除します。

例

次に、実行コンフィギュレーションから **multicast-routing** コマンドを削除する例を示します。

```
hostname(config)# clear configure multicast-routing
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

clear configure nac-policy

実行コンフィギュレーションから、すべての NAC ポリシー（グループ ポリシーに割り当てられている NAC ポリシーを除く）を削除するには、グローバル コンフィギュレーション モードで **clear configure nac-policy** コマンドを使用します。

clear configure nac-policy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべての NAC ポリシーを削除する場合にのみ使用します。コンフィギュレーションから 1 つの NAC ポリシーを削除するには、nac-policy コマンドの **no** 形式を使用します。

例

次のコマンドは、すべての NAC ポリシーを削除する方法を示しています。

```
hostname(config)# clear config nac-policy
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show running-config nac-policy	セキュリティ アプライアンス上の各 NAC ポリシーのコンフィギュレーションを表示します。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

clear configure name

コンフィギュレーションから名前のリストをクリアするには、グローバル コンフィギュレーション モードで **clear configure name** コマンドを使用します。

clear configure name

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、名前のリストをクリアする例を示します。

```
hostname(config)# clear configure name
```

関連コマンド

コマンド	説明
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。

clear configure nat

NAT コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure nat** コマンドを使用します。

clear configure nat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

使用上のガイドライン

次のことが、トランスペアレント ファイアウォール モードに適用されます。

（注）　トランスペアレント ファイアウォール モードでは、NAT ID 0 のみが有効です。

例

次に、NAT コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure nat
```

関連コマンド

コマンド	説明
nat	ネットワークをグローバル IP アドレス プールに関連付けます。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

clear configure nat-control

NAT コンフィギュレーションの要件をディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure nat-control** コマンドを使用します。

clear configure nat-control

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、NAT コンフィギュレーションの要件をディセーブルにする例を示します。

```
hostname(config)# clear configure nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
nat-control	NAT コントロールを適用します。NAT コントロールをディセーブルにすると、NAT ルールを設定することなく、内部ホストが外部ネットワークと通信できます。
show running-config nat-control	NAT コンフィギュレーションの要件を表示します。

clear configure ntp

NTP コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure ntp** コマンドを使用します。

clear configure ntp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear ntp** から変更されました。

例

次に、すべての **ntp** コマンドをクリアする例を示します。

```
hostname# clear configure ntp
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP 認証キーを設定します。
ntp server	セキュリティ アプライアンスの時間を設定する NTP サーバを指定します。
ntp trusted-key	NTP の信頼できるキーを指定します。
show running-config ntp	NTP コンフィギュレーションを表示します。

clear configure object-group

コンフィギュレーションからすべての **object group** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure object-group** コマンドを使用します。

clear configure object-group [**protocol** | **service** | **icmp-type** | **network**]

構文の説明

icmp-type	（任意）すべての ICMP グループをクリアします。
network	（任意）すべてのネットワーク グループをクリアします。
protocol	（任意）すべてのプロトコル グループをクリアします。
service	（任意）すべてのサービス グループをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、コンフィギュレーションからすべての **object-group** コマンドを削除する例を示します。

```
hostname(config)# clear configure object-group
```

関連コマンド

コマンド	説明
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

clear configure passwd

ログイン パスワード コンフィギュレーションをクリアし、デフォルト設定の「cisco」に戻すには、グローバル コンフィギュレーション モードで **clear configure passwd** コマンドを使用します。

clear configure {**passwd** | **password**}

構文の説明

passwd	**password**	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear passwd** から変更されました。

例

次に、ログイン パスワードをクリアし、デフォルトの「cisco」に戻す例を示します。

```
hostname(config)# clear configure passwd
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config passwd	暗号化された形式でログイン パスワードを表示します。

clear configure phone-proxy

電話プロキシ コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure phone-proxy** コマンドを使用します。

clear configure phone-proxy [*phone_proxy_name*]

構文の説明

phone_proxy_name	Phone Proxy インスタンスの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**clear configure phone-proxy** コマンドを使用して、電話プロキシ コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure phone-proxy asa_phone_proxy
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

clear configure pim

実行コンフィギュレーションからすべてのグローバル **pim** コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure pim** コマンドを使用します。

clear configure pim

構文の説明

このコマンドには、キーワードや引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure pim コマンドは、実行コンフィギュレーションからすべての **pim** コマンドをクリアします。PIM トラフィック カウンタおよびトポロジ情報をクリアするには、**clear pim counters** コマンドおよび **clear pim topology** コマンドを使用します。

clear configure pim コマンドはグローバル コンフィギュレーション モードで入力された **pim** コマンドだけをクリアします。インターフェイス固有の **pim** はクリアしません。

例

次に、実行コンフィギュレーションからすべての **pim** コマンドをクリアする例を示します。

```
hostname(config)# clear configure pim
```

関連コマンド

コマンド	説明
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。
show running-config pim	実行コンフィギュレーション内の **pim** コマンドを表示します。

clear configure policy-map

すべての **policy-map** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure policy-map** コマンドを使用します。

clear configure policy-map [**type inspect** [*protocol*]}

構文の説明

type inspect	（任意）インスペクション ポリシー マップをクリアします。
protocol	（任意）クリアするインスペクション ポリシー マップのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　特定の名前のポリシー マップをクリアするには、**policy-map** コマンドの **no** 形式を使用します。

例　次に、**clear configure policy-map** コマンドの例を示します。

```
hostname(config)# clear configure policy-map
```

関連コマンド

コマンド	説明
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	ポリシー コンフィギュレーション全体を表示します。

clear configure pop3s

コンフィギュレーションからすべての POP3S コマンドを削除して、デフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure pop3s** コマンドを使用します。

clear configure pop3s

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、POP3S コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure pop3s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration pop3s	POP3S の実行コンフィギュレーションを表示します。
pop3s	POP3S 電子メール プロキシ コンフィギュレーションを作成または編集します。

clear configure prefix-list

実行コンフィギュレーションから **prefix-list** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure prefix-list** コマンドを使用します。

clear configure prefix-list [*prefix_list_name*]

構文の説明

prefix_list_name	（任意）プレフィックス リストの名前。プレフィックス リスト名を指定した場合は、そのプレフィックス リストのコマンドだけがコンフィギュレーションから削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear prefix-list** から **clear configure prefix-list** に変更されました。

使用上のガイドライン

clear configure prefix-list コマンドは、実行コンフィギュレーションから **prefix-list** コマンドと **prefix-list description** コマンドを削除します。プレフィックス リスト名を指定した場合は、実行コンフィギュレーションからそのプレフィックス リストの **prefix-list** コマンドと **prefix-list description** コマンド（存在する場合）だけが削除されます。

このコマンドは、実行コンフィギュレーションから **no prefix-list sequence** コマンドを削除しません。

例

次に、実行コンフィギュレーションから、MyPrefixList という名前のプレフィックス リストの、すべての **prefix-list** コマンドを削除する例を示します。

```
hostname# clear configure prefix-list MyPrefixList
```

関連コマンド

コマンド	説明
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

clear configure priority-queue

コンフィギュレーションからプライオリティ キューの指定を削除するには、グローバル コンフィギュレーション モードで **clear configure priority-queue** コマンドを使用します。

clear configure priority queue *interface-name*

構文の説明

interface-name	プライオリティ キューの詳細を表示するインターフェイスの名前を指定します。

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**clear configure priority-queue** コマンドを使用して、test という名前のインターフェイスのプライオリティ キュー コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure priority-queue test
```

関連コマンド

コマンド	説明
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear configure privilege

コマンドの設定済み特権レベルを削除するには、グローバル コンフィギュレーション モードで **clear configure privilege** コマンドを使用します。

clear configure privilege

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

取り消し操作はありません。

例

次に、コマンドの設定済み特権レベルをリセットする例を示します。

```
hostname(config)# clear configure privilege
```

関連コマンド

コマンド	説明
privilege	コマンド特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

clear configure regex

すべての正規表現を削除するには、グローバル コンフィギュレーション モードで **clear configure regex** コマンドを使用します。

clear configure regex

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定の名前の正規表現をクリアするには、**regex** コマンドの **no** 形式を使用します。

例

次に、設定済みのすべての正規表現をクリアする例を示します。

```
hostname(config)# clear configure regex
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。
show running-config regex	すべての正規表現を表示します。
test regex	正規表現をテストします。

clear configure route

connect キーワードを含まないコンフィギュレーションから **route** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure route** コマンドを使用します。

clear configure route [*interface_name ip_address* [*netmask gateway_ip*]]

構文の説明

gateway_ip	（任意）ゲートウェイ ルータの IP アドレスを指定します（このルートのネクスト ホップ アドレス）。
interface_name	（任意）内部または外部のネットワーク インターフェイス名。
ip_address	（任意）内部または外部ネットワーク IP アドレス。
netmask	（任意）*ip_address* に適用するネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

使用上のガイドライン

デフォルト ルートを指定するには、**0.0.0.0** を使用します。0.0.0.0 IP アドレスは **0** に、0.0.0.0 *netmask* は **0** に省略できます。

例

次に、**connect** キーワードを含まないコンフィギュレーションから **route** コマンドを削除する例を示します。

```
hostname(config)# clear configure route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear configure route-map

すべてのルート マップを削除するには、グローバル コンフィギュレーション モードで **clear configure route-map** コマンドを使用します。

clear configure route-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンフィギュレーション内のすべての **route-map** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure route-map** コマンドを使用します。**route-map** コマンドは、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を設定するために使用されます。

route-map コマンドを個別に削除するには、**no route-map** コマンドを使用します。

例

次に、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除する例を示します。

```
hostname(config)# clear configure route-map
```

関連コマンド

コマンド	説明
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
show running-config route-map	ルート マップ コンフィギュレーションに関する情報を表示します。

clear configure router

実行コンフィギュレーションからルータ コンフィギュレーション コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure router** コマンドを使用します。

clear configure router [**ospf** [*id*] | **rip** | **eigrp** [*as-number*]]

構文の説明

as-number	（任意）指定した EIGRP 自律システム番号（プロセス ID とも呼びます）に対するコンフィギュレーション コマンドをクリアします。指定しないと、すべての EIGRP ルーティング プロセスに対するコンフィギュレーション コマンドがクリアされます。値の範囲は 1 ～ 65535 です。 セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、オプションの *as-number* 引数を含めても、省略した場合と同じ結果になります。
eigrp	（任意）コンフィギュレーションから EIGRP ルータ コンフィギュレーション コマンドだけを削除することを指定します。EIGRP インターフェイス コンフィギュレーション モード コマンドは削除されません。
id	（任意）指定した OSPF プロセス ID のコンフィギュレーション コマンドをクリアします。ID を指定しないと、すべての OSPF プロセスのコンフィギュレーション コマンドがクリアされます。
ospf	（任意）コンフィギュレーションから OSPF コンフィギュレーション コマンドだけを削除することを指定します。
rip	コンフィギュレーションから RIP コンフィギュレーション コマンドだけを削除することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear router** コマンドから **clear configure router** コマンドに変更されました。
7.2(1)	**rip** キーワードがコマンドに追加されました。
8.0(2)	**eigrp** キーワードがコマンドに追加されました。

例

次に、実行コンフィギュレーションから、OSPF プロセス 1 に関連付けられているすべての OSPF コマンドをクリアする例を示します。

```
hostname(config)# clear configure router ospf 1
```

次に、実行コンフィギュレーションから、RIP ルーティング プロセスに関連付けられているすべてのグローバル コンフィギュレーション モード コマンドをクリアする例を示します。インターフェイス コンフィギュレーション モードで入力された RIP コマンドはクリアされません。

```
hostname(config)# clear configure router rip
```

関連コマンド

コマンド	説明
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
router ospf	OSPF ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。

clear configure same-security-traffic

same-security-traffic コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure same-security-traffic** コマンドを使用します。

clear configure same-security-traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**same-security-traffic** コマンドが発行されたときにコンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure same-security-traffic
```

関連コマンド

コマンド	説明
same-security-traffic	同じセキュリティ レベルのインターフェイス間の通信を許可します。
show running-config same-security-traffic	**same-security-traffic** コマンドが発行されたときにコンフィギュレーションを表示します。

clear configure service-policy

サービス ポリシー コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure service-policy** コマンドを使用します。

clear configure service-policy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**clear configure service-policy** コマンドの例を示します。

```
hostname(config)# clear configure service-policy
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
service-policy	サービス ポリシーを設定します。
clear service-policy	サービス ポリシーの統計情報をクリアします。

clear configure sla monitor

実行コンフィギュレーションから **sla monitor** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure sla monitor** コマンドを使用します。

clear configure sla monitor [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id を指定しなかった場合、SLA 動作のコンフィギュレーションがすべてクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**sla monitor** コマンド、関連する SLA モニタ コンフィギュレーション モード コマンド、および関連する **sla monitor** schedule コマンド（存在する場合）をクリアします。**track rtr** コマンドは、コンフィギュレーションから削除されません。

実行コンフィギュレーション内の sla monitor コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次に、コンフィギュレーションからすべての **sla monitor** コマンドをクリアする例を示します。

```
hostname(config)# clear configure sla monitor
```

次に、SLA 動作 ID 5 に関連付けられている **sla monitor** コマンドをクリアする例を示します。

```
hostname(config)# clear configure sla monitor 5
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーション内の sla monitor コマンドを表示します。

clear configure smtps

コンフィギュレーションからすべての SMTPS コマンドを削除して、デフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure smtps** コマンドを使用します。

clear configure smtps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、SMTPS コンフィギュレーションを削除する例を示します。

```
hostname(config)# clear configure smtps
```

関連コマンド

コマンド	説明
show running-configuration smtps	SMTPS の実行コンフィギュレーションを表示します。
smtps	SMTPS 電子メール プロキシ コンフィギュレーションを作成または編集します。

clear configure smtp-server

SMTP サーバのコマンドと統計情報をすべてクリアするには、グローバル コンフィギュレーション モードで **clear configure smtp-server** コマンドを使用します。

clear configure smtp-server

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

clear configure smtp-server コマンドは、**smtp** コマンドおよび統計情報をすべてクリアします。

例

次に、すべての **smtp-server** コマンドをクリアする例を示します。

```
hostname(config)# clear configure smtp-server
```

関連コマンド

コマンド	説明
show running-config smtp-server	現在の DHCP サーバ コンフィギュレーションを表示します。

clear configure snmp-map

SNMP マップ コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure snmp-map** コマンドを使用します。

clear configure snmp-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure snmp-map コマンドは、SNMP マップ コンフィギュレーションを削除します。

例

次に、SNMP マップ コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure snmp-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

clear configure snmp-server

SNMP サーバをディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure snmp-server** コマンドを使用します。

clear configure snmp-server

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

この例は、SNMP サーバをディセーブルにする方法を示しています。

```
hostname# clear configure snmp-server
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
show snmp-server statistics	SNMP サーバのコンフィギュレーションに関する情報を表示します。

clear configure ssh

実行コンフィギュレーションからすべての SSH コマンドをクリアするには、グローバル コンフィギュレーション モードで **clear configure ssh** コマンドを使用します。

clear configure ssh

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear ssh** コマンドから **clear configure ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションからすべての SSH コマンドをクリアします。特定のコマンドをクリアするには、このコマンドの **no** 形式を使用します。

例

次に、コンフィギュレーションからすべての SSH コマンドをクリアする例を示します。

```
hostname(config)# clear configure ssh
```

関連コマンド

コマンド	説明
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh scopy enable	セキュリティ アプライアンスでセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

clear configure ssl

コンフィギュレーションからすべての SSL コマンドを削除して、デフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure ssl** コマンドを使用します。

clear configure ssl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトは次のとおりです。

- SSL クライアントおよび SSL サーバのバージョンは両方とも **any** です。
- SSL 暗号化は、3des-sha1 | des-sha1 | rc4-md5 の順番です。
- トラストポイント アソシエーションはありません。セキュリティ アプライアンスはデフォルトの RSA キー ペア証明書を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**clear configure ssl** コマンドの使用例を示します。

```
hostname(config)# clear configure ssl
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

clear configure static

コンフィギュレーションからすべての **static** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure static** コマンドを使用します。

clear configure static

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

例

次に、コンフィギュレーションからすべての **static** コマンドを削除する例を示します。

```
hostname(config)# clear configure static
```

関連コマンド

コマンド	説明
show running-config static	コンフィギュレーション内のすべての **static** コマンドを表示します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定します。

clear configure sunrpc-server

リモート プロセッサ コール サービスをセキュリティ アプライアンスからクリアするには、グローバル コンフィギュレーション モードで **clear configure sunrpc-server** コマンドを使用します。

clear configure sunrpc-server [**active**]

構文の説明

active	（任意）セキュリティ アプライアンスで現在アクティブな SunRPC サービスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

sunrpc-server コマンドは、設定済みの **router ospf** コマンドを表示します。

（注） セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスである場合、このアドレスは hello パケットおよびデータベース定義で送信されます。このアクションを防止するには、**router-id** *ip_address* をグローバル アドレスに設定します。

例

次に、セキュリティ アプライアンスから SunRPC サービスをクリアする例を示します。

```
hostname(config)# clear configure sunrpc-server active
```

関連コマンド

コマンド	説明
sunrpc-server	SunRPC サービス テーブルを作成します。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

clear configure sysopt

すべての **sysopt** コマンドのコンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure sysopt** コマンドを使用します。

clear configure sysopt

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear sysopt** から変更されました。

例

次に、すべての **sysopt** コマンドのコンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure sysopt
```

関連コマンド

コマンド	説明
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

clear configure tcp-map

tcp-map コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure tcp-map** コマンドを使用します。

clear configure tcp-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、TCP マップ コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure tcp-map
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。

clear configure telnet

コンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除するには、グローバル コンフィギュレーション モードで **clear configure telnet** コマンドを使用します。

clear configure telnet

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **configure** が追加されました。

例

次に、セキュリティ アプライアンスのコンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除する例を示します。

```
hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

clear configure terminal

端末の表示幅設定をクリアするには、グローバル コンフィギュレーション モードで **clear configure terminal** コマンドを使用します。

clear configure terminal

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**configure** キーワードが追加されました。

例

次に、表示幅をクリアする例を示します。

```
hostname# clear configure terminal
```

関連コマンド

コマンド	説明
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。
show running-config terminal	現在の端末設定を表示します。

clear configure threat-detection

脅威検出コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure threat-detection** コマンドを使用します。

clear configure threat-detection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべての **threat-detection** コンフィギュレーション コマンドをクリアします。

例

次に、すべての脅威検出コマンドをクリアする例を示します。

```
hostname# clear configure threat-detection
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
clear threat-detection shun	現在回避されているホストを解放します。
show running-config threat-detection	脅威検出コンフィギュレーションを表示します。
threat-detection basic-threat	基本的な脅威の検出をイネーブルにします。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear configure timeout

コンフィギュレーションのデフォルトのアイドル時間に戻すには、グローバル コンフィギュレーション モードで **clear configure timeout** コマンドを使用します。

clear configure timeout

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、コンフィギュレーションから最大アイドル時間を削除する例を示します。

```
hostname(config)# clear configure timeout
```

関連コマンド

コマンド	説明
show running-config timeout	指定されたプロトコルのタイムアウト値を表示します。
timeout	アイドル時間の最大継続期間を設定します。

clear configure time-range

設定されているすべての時間範囲をクリアするには、グローバル コンフィギュレーション モードで **clear configure time-range** コマンドを使用します。

clear configure time-range

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、設定済みのすべての時間範囲をクリアする例を示します。

```
hostname(config)# clear configure time-range
```

関連コマンド

コマンド	説明
time-range	時間範囲コンフィギュレーション モードを開始し、トラフィック ルールまたはアクションに付加できる時間範囲を定義します。

clear configure tls-proxy

設定されているすべての TLS プロキシ インスタンスを削除するには、グローバル コンフィギュレーション モードで **clear configure tls-proxy** コマンドを使用します。

clear configure tls-proxy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**clear configure tls-proxy** コマンドを使用して、設定されているすべての TLS プロキシ インスタンスを削除する例を示します。

```
hostname# clear configure tls-proxy
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show running-config tls-proxy	すべてまたは指定された TLS プロキシの実行コンフィギュレーションを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

clear configure tunnel-group

コンフィギュレーションからすべてのトンネル グループまたは指定したトンネル グループを削除するには、グローバル コンフィギュレーションで **clear config tunnel-group** コマンドを使用します。

clear config tunnel-group [*name*]

構文の説明

name	（任意）トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、コンフィギュレーションから toengineering トンネル グループを削除する例を示します。

```
hostname(config)# clear config tunnel-group toengineering
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config tunnel-group	すべてのトンネル グループまたは選択したトンネル グループに関する情報を表示します。
tunnel-group	指定されたタイプのトンネル グループ サブコンフィギュレーション モードを開始します。

clear configure tunnel-group-map

clear configure tunnel-group-map コマンドは、証明書のコンテンツからトンネル グループ名が生成されるときに使用されるポリシーおよびルールをクリアします。

clear configure tunnel-group-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ ルールもこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は group1 です。

```
hostname(config)# clear configure tunnel-group-map
```

関連コマンド

コマンド	説明
crypto ca certificate map	暗号 CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルトのトンネル グループとして指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。

clear configure url-block

URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure url-block** コマンドを使用します。

clear configure url-block

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-block コマンドは、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションをクリアします。

例

次に、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure url-block
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure url-cache

URL キャッシュをクリアするには、グローバル コンフィギュレーション モードで **clear configure url-cache** コマンドを使用します。

clear configure url-cache

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-cache コマンドは、URL キャッシュをクリアします。

例

次に、URL キャッシュをクリアする例を示します。

```
hostname# clear configure url-cache
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**scsc** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure url-list

WebVPN ユーザがアクセスできる設定済みの URL のセットを削除するには、グローバル コンフィギュレーション モードで **clear configure url-list** コマンドを使用します。設定済みのすべての URL を削除するには、このコマンドを *listname* 引数なしで使用します。特定のリストの URL だけを削除するには、*listname* を指定してこのコマンドを使用します。

clear configure url-list [*listname***]**

構文の説明

listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、*Marketing URLs* という URL リストを削除する例を示します。

```
hostname(config)# clear configure url-list Marketing URLs
```

関連コマンド

コマンド	説明
show running-configuration url-list	現在設定されている一連の **url-list** コマンドを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、グローバル コンフィギュレーション モードでこのコマンドを使用します。
url-list	特定のグループ ポリシーまたはユーザの WebVPN URL アクセスをイネーブルにするには、グループ ポリシーまたはユーザ名モードからアクセスする webvpn モードでこのコマンドを使用します。

clear configure url-server

URL フィルタリング サーバ コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure url-server** コマンドを使用します。

clear configure url-server

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-server コマンドは、URL フィルタリング サーバ コンフィギュレーションをクリアします。

例

次に、URL フィルタリング サーバ コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure url-server
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure username

ユーザ名データベースをクリアするには、グローバル コンフィギュレーション モードで **clear configure username** コマンドを使用します。特定のユーザのコンフィギュレーションをクリアするには、このコマンドを使用し、ユーザ名を付加します。

clear configure username [*name*]

構文の説明

name	（任意）ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドでは、このデータベースを認証用に使用します。

例

次に、anyuser という名前のユーザのコンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure username anyuser
```

関連コマンド

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	特定のユーザの AVP を設定できます。

clear configure virtual

コンフィギュレーションから認証仮想サーバを削除するには、グローバル コンフィギュレーション モードで **clear configure virtual** コマンドを使用します。

clear configure virtual

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

取り消し操作はありません。

例

次に、**clear configure virtual** コマンドの例を示します。

```
hostname(config)# clear configure virtual
```

関連コマンド

コマンド	説明
show running-config virtual	認証仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンスと HTTP サーバでの別々の認証を可能にします。
virtual telnet	セキュリティ アプライアンスが認証プロンプトを提供しないトラフィック タイプの仮想 Telnet サーバでユーザを認証します。

clear configure vpdn group

コンフィギュレーションからすべての **vpdn group** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure vpdn group** コマンドを使用します。

clear configure vpdn group

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpdn group コマンドを入力しても、アクティブな PPPoE 接続に影響はありません。

例

次に、VPDN グループ コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure vpdn group
```

関連コマンド

コマンド	説明
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

clear configure vpdn username

コンフィギュレーションからすべての **vpdn username** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure vpdn username** コマンドを使用します。

clear configure vpdn username

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpdn username コマンドを入力しても、アクティブな PPPoE 接続に影響はありません。

例

次に、VPDN ユーザ名コンフィギュレーションをクリアする例を示します。

```
hostname(config)# clear configure vpdn username
```

関連コマンド

コマンド	説明
clear configure vpdn group	コンフィギュレーションからすべての vpdn group コマンドを削除します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

clear configure vpn-load-balancing

以前に指定した VPN ロード バランシング コンフィギュレーションを削除して、VPN ロード バランシングをディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure vpn load-balancing** コマンドを使用します。

clear configure vpn load-balancing

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpn load-balancing コマンドは、**cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、**priority** などの関連コマンドもクリアします。

例

次のコマンドでは、コンフィギュレーションから VPN ロード バランシング コンフィギュレーション ステートメントを削除しています。

```
hostname(config)# clear configure vpn load-balancing
```

関連コマンド

show running-config load-balancing	現在の VPN ロード バランシング コンフィギュレーションを表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

clear configure wccp

すべての WCCP 設定を削除するには、グローバル コンフィギュレーション モードで **clear configure wccp** コマンドを使用します。

clear configure wccp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、WCCP 設定をクリアする例を示します。

```
hostname(config)# clear configure wccp
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear configure zonelabs-integrity

実行コンフィギュレーションからすべての Zone Labs Integrity サーバを削除するには、グローバル コンフィギュレーション モードで **clear configure zonelabs-integrity** コマンドを使用します。

clear configure zonelabs-integrity

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

すべての Zone Labs Integrity サーバを削除します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure zonelabs-integrity コマンドは、実行コンフィギュレーションからすべての Zone Labs Integrity サーバ（アクティブとスタンバイを含む）を削除します。

例

次に、設定済みの 2 つの Zone Labs Integrity サーバを削除する例を示します。

```
hostname(config)# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
hostname(config)# clear configure zonelabs-integrity
hostname(config)# show running-config zonelabs-integrity
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config [all] zonelabs-integrity	設定されている Zone Labs Integrity サーバを表示します。

CHAPTER 7

clear conn コマンド～ clear xlate コマンド

clear conn

特定の接続または複数の接続をクリアするには、特権 EXEC モードで **clear conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]]
[**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]]
[**port** *dest_port*[**-***dest_port*]]

構文の説明

address	（任意）指定された送信元または宛先の IP アドレスとの接続をクリアします。
all	（任意）デバイスを通過するトラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を消去します。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定された送信元または宛先のポートとの接続をクリアします。
protocol {tcp | udp}	（任意）プロトコル **tcp** または **udp** との接続をクリアします。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスで第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

例

次に、すべての接続を表示し、次に 10.10.10.108:4168 と 10.0.8.112:22 間の管理接続をクリアする例を示します。

```
hostname# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

hostname# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

関連コマンド

コマンド	説明
clear local-host	特定のローカル ホストまたはすべてのローカル ホストによるすべての接続をクリアします。
clear xlate	NAT セッション、または NAT を使用した任意の接続を消去します。
show conn	接続情報を表示します。
show local-host	ローカル ホストのネットワーク状態を表示します。
show xlate	NAT セッションを表示します。

clear console-output

現在キャプチャされているコンソール出力を削除するには、特権 EXEC モードで **clear console-output** コマンドを使用します。

clear console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、現在キャプチャされているコンソール出力を削除する例を示します。

```
hostname# clear console-output
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
show console-output	キャプチャされているコンソール出力を表示します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

clear counters

プロトコル スタック カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear counters** コマンドを使用します。

clear counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

構文の説明

all	（任意）すべてのフィルタ詳細をクリアします。
context *context-name*	（任意）コンテキスト名を指定します。
:*counter_name*	（任意）名前でカウンタを指定します。
detail	（任意）カウンタの詳細情報をクリアします。
protocol *protocol_name*	（任意）指定したプロトコルのカウンタをクリアします。
summary	（任意）カウンタの要約をクリアします。
threshold *N*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。
top *N*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、プロトコル スタック カウンタをクリアする例を示します。

```
hostname(config)# clear counters
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

clear crashinfo

フラッシュ メモリ内のクラッシュ ファイルの内容を削除するには、特権 EXEC モードで **clear crashinfo** コマンドを使用します。

clear crashinfo

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次のコマンドは、クラッシュ ファイルの削除方法を示しています。

```
hostname# clear crashinfo
```

関連コマンド

crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示します。

clear crypto accelerator statistics

クリプト アクセラレータ MIB からグローバルな統計情報およびアクセラレータ固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto accelerator statistics** コマンドを使用します。

clear crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear crypto ca crls

指定したトラストポイントに関連付けられているすべての CRL の CRL キャッシュ、またはすべての CRL の CRL キャッシュを削除するには、特権 EXEC モードで **clear crypto ca crls** コマンドを使用します。

clear crypto ca crls [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべてクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで発行され、セキュリティ アプライアンスからすべての CRL のすべての CRL キャッシュを削除する例を示します。

```
hostname# clear crypto ca crls
hostname#
```

関連コマンド

コマンド	説明
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crls	キャッシュされたすべての CRL、または指定したトラストポイントのキャッシュされた CRL を表示します。

clear crypto ipsec sa

IPSec SA のカウンタ、エントリ、クリプト マップ、またはピア接続を削除するには、特権 EXEC モードで **clear crypto ipsec sa** コマンドを使用します。すべての IPSec SA をクリアするには、このコマンドを引数なしで使用します。

clear [crypto] ipsec sa [counters | entry {*hostname* | *ip_address*} **{esp | ah}** *spi* **| map** *map name* **| peer** {*hostname* | *ip_address*}**]**

このコマンドを使用するときは注意してください。

構文の説明

ah	認証ヘッダー。
counters	各 SA 統計情報のすべての IPSec をクリアします。
entry	指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。
esp	暗号化セキュリティ プロトコル。
hostname	IP アドレスに割り当てられたホスト名を指定します。
ip_address	IP アドレスを指定します。
map	マップ名で識別される、指定したクリプト マップに関連付けられているすべてのトンネルを削除します。
map name	クリプト マップを識別する英数字ストリング。最大 64 文字です。
peer	指定したホスト名または IP アドレスで識別されるピアへのすべての IPSec SA を削除します。
spi	セキュリティ パラメータ インデックス（16 進数）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、セキュリティ アプライアンスからすべての IPSec SA を削除する例を示します。

```
hostname# clear crypto ipsec sa
hostname#
```

次に、グローバル コンフィギュレーション モードで、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
hostname# clear crypto ipsec peer 10.86.1.1
hostname#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPSec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など暗号コンフィギュレーション全体を表示します。

clear crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto protocol statistics** コマンドを使用します。

clear crypto protocol statistics *protocol*

構文の説明

protocol	統計情報をクリアするプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 • **ikev1**：インターネット キー交換バージョン 1。 • **ipsec**：IP セキュリティ フェーズ 2 プロトコル。 • **ssl**：Secure Socket Layer。 • **other**：新規プロトコル用に予約済み。 • **all**：現在サポートされているすべてのプロトコル。 このコマンドのオンライン ヘルプでは、今後のリリースでサポートされる他のプロトコルが表示される場合があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、すべてのクリプト アクセラレータの統計情報をクリアする例を示します。

```
hostname# clear crypto protocol statistics all
hostname#
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。

コマンド	説明
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	クリプト アクセラレータ MIB のプロトコル固有の統計情報を表示します。

clear dhcpd

DHCP サーバのバインディングおよび統計情報をクリアするには、特権 EXEC モードで **clear dhcp** コマンドを使用します。

clear dhcpd {**binding** [*ip_address*] | **statistics**}

構文の説明

binding	クライアント アドレスのすべてのバインディングをクリアします。
ip_address	（任意）指定した IP アドレスのバインディングをクリアします。
statistics	統計情報カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

オプションの IP アドレスを **clear dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけがクリアされます。

すべての DHCP サーバ コマンドをクリアするには、**clear configure dhcpd** コマンドを使用します。

例

次に、**dhcpd** 統計情報をクリアする例を示します。

```
hostname# clear dhcpd statistics
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

clear dhcprelay statistics

DHCP リレー統計情報カウンタをクリアするには、特権 EXEC モードで **clear dhcprelay statistics** コマンドを使用します。

clear dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear dhcprelay statistics コマンドは、DHCP リレー統計情報カウンタだけをクリアします。DHCP リレー コンフィギュレーション全体をクリアするには、**clear configure dhcprelay** コマンドを使用します。

例

次に、DHCP リレー統計情報をクリアする例を示します。

```
hostname# clear dhcprelay statistics
hostname#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

clear dns-hosts cache

DNS キャッシュをクリアするには、特権 EXEC モードで **clear dns-hosts cache** コマンドを使用します。このコマンドは、**name** コマンドで追加したスタティック エントリをクリアしません。

clear dns-hosts cache

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、DNS キャッシュをクリアする例を示します。

```
hostname# clear dns-hosts cache
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear eigrp events

EIGRP イベント ログをクリアするには、特権 EXEC モードで **clear eigrp events** コマンドを使用します。

clear eigrp [*as-number*] **events**

構文の説明

as-number	（任意）イベント ログをクリアする EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show eigrp events コマンドを使用して、EIGRP イベント ログを表示できます。

例

次に、EIGRP イベント ログをクリアする例を示します。

```
hostname# clear eigrp events
```

関連コマンド

コマンド	説明
show eigrp events	EIGRP イベント ログを表示します。

clear eigrp neighbors

EIGRP ネイバー テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp neighbors** コマンドを使用します。

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、このインターフェイスを介して学習されたすべてのネイバー テーブル エントリが削除されます。
ip-addr	（任意）ネイバー テーブルから削除するネイバーの IP アドレス。
soft	セキュリティ アプライアンスは、隣接関係をリセットすることなくネイバーと再同期されます。

デフォルト

ネイバー IP アドレスまたはインターフェイス名を指定しない場合は、すべてのダイナミック エントリがネイバー テーブルから削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp neighbors コマンドは、**neighbor** コマンドを使用して定義されたネイバーをネイバー テーブルから削除しません。ダイナミックに検出されたネイバーだけが削除されます。

show eigrp neighbors コマンドを使用して、EIGRP ネイバー テーブルを表示できます。

例

次に、EIGRP ネイバー テーブルからすべてのエントリを削除する例を示します。

```
hostname# clear eigrp neighbors
```

次に、「outside」という名前のインターフェイスを介して学習されたすべてのエントリを EIGRP ネイバー テーブルから削除する例を示します。

```
hostname# clear eigrp neighbors outside
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバーのデバッグ情報を表示します。
debug ip eigrp	EIGRP プロトコル パケットのデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

clear eigrp topology

EIGRP トポロジ テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp topology** コマンドを使用します。

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

構文の説明

as-number	（任意）EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。
ip-addr	トポロジ テーブルからクリアする IP アドレス。
mask	（任意）*ip-addr* 引数に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、EIGRP トポロジ テーブルから既存の EIGRP エントリをクリアします。**show eigrp topology** コマンドを使用して、トポロジ テーブルのエントリを表示できます。

例

次に、EIGRP トポロジ テーブルから 192.168.1.0 ネットワークのエントリを削除する例を示します。

```
hostname# clear eigrp topology 192.168.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp topology	EIGRP トポロジ テーブルを表示します。

clear failover statistics

フェールオーバー統計情報カウンタをクリアするには、特権 EXEC モードで **clear failover statistics** コマンドを使用します。

clear failover statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**show failover statistics** コマンドで表示される統計情報、および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタをクリアします。フェールオーバー コンフィギュレーションを削除するには、**clear configure failover** コマンドを使用します。

例

次に、フェールオーバー統計情報カウンタをクリアする例を示します。

```
hostname# clear failover statistics
hostname#
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー デバッグ情報を表示します。
show failover	フェールオーバー コンフィギュレーションおよび動作統計に関する情報を表示します。

clear fragment

IP フラグメント再構築モジュールの動作データをクリアするには、特権 EXEC モードで **clear fragment** コマンドを入力します。このコマンドは、現在キューに入っている再構築待機中のフラグメント（**queue** キーワードが入力されている場合）、またはすべての IP フラグメント再構築統計情報（**statistics** キーワードが入力されている場合）のいずれかをクリアします。統計情報は、再構築に成功したフラグメント チェーンの数、再構築に失敗したチェーンの数、および最大サイズの超過によってバッファ オーバーフローが発生した回数を示すカウンタです。

clear fragment {**queue** | **statistics**} [*interface*]

構文の説明

interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。
queue	IP フラグメント再構築キューをクリアします。
statistics	IP フラグメント再構築統計情報をクリアします。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データのクリアを動作データのクリアと区別するために、**clear fragment** および **clear configure fragment** という 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データをクリアする例を示します。

```
hostname# clear fragment queue
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear gc

ガーベッジ コレクション プロセスの統計情報を削除するには、特権 EXEC モードで **clear gc** コマンドを使用します。

clear gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ガーベッジ コレクション プロセスの統計情報を削除する例を示します。

```
hostname# clear gc
```

関連コマンド

コマンド	説明
show gc	ガーベッジ コレクション プロセスの統計情報を表示します。

clear igmp counters

すべての IGMP カウンタをクリアするには、特権 EXEC モードで **clear igmp counters** コマンドを使用します。

clear igmp counters [*if_name*]

構文の説明

if_name	**nameif** コマンドで指定されたインターフェイス名。このコマンドにインターフェイス名を含めると、指定したインターフェイスのカウンタだけがクリアされます。

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IGMP 統計情報カウンタをクリアする例を示します。

```
hostname# clear igmp counters
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp group

検出されたグループを IGMP グループ キャッシュからクリアするには、特権 EXEC モードで **clear igmp** コマンドを使用します。

clear igmp group [*group* | **interface** *name*]

構文の説明

group	IGMP グループ アドレス。特定のグループを指定すると、そのグループがキャッシュから削除されます。
interface *name*	**namif** コマンドで指定されたインターフェイス名。指定した場合は、そのインターフェイスに関連付けられたすべてのグループが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

グループまたはインターフェイスを指定しない場合は、すべてのインターフェイスからすべてのグループがクリアされます。グループを指定した場合は、そのグループのエントリだけがクリアされます。インターフェイスを指定した場合は、そのインターフェイスのすべてのグループがクリアされます。グループとインターフェイスの両方を指定した場合は、指定したインターフェイスの指定したグループだけがクリアされます。

このコマンドは、スタティックに設定されたグループをクリアしません。

例

次に、検出されたすべての IGMP グループを IGMP グループ キャッシュからクリアする例を示します。

```
hostname# clear igmp group
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp traffic

IGMP トラフィック カウンタをクリアするには、特権 EXEC モードで **clear igmp traffic** コマンドを使用します。

clear igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IGMP 統計情報トラフィック カウンタをクリアする例を示します。

```
hostname# clear igmp traffic
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp counters	すべての IGMP カウンタをクリアします。

clear interface

インターフェイス統計情報をクリアするには、特権 EXEC モードで **clear interface** コマンドを使用します。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

インターフェイスがコンテキスト間で共有されている場合にコンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストの統計情報だけをクリアします。システム実行スペースでこのコマンドを入力した場合、セキュリティ アプライアンスは結合された統計情報をクリアします。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。

例

次に、すべてのインターフェイス統計情報をクリアする例を示します。

```
hostname# clear interface
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイスの設定を表示します。

clear ip audit count

監査ポリシーのシグニチャ一致の数をクリアするには、特権 EXEC モードで **clear ip audit count** コマンドを使用します。

clear ip audit count [**global** | **interface** *interface_name*]

構文の説明

global	（デフォルト）すべてのインターフェイスの一致数をクリアします。
interface *interface_name*	（任意）指定したインターフェイスの一致数をクリアします。

デフォルト

キーワードを指定しない場合、このコマンドはすべてのインターフェイスの一致をクリアします（**global**）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、すべてのインターフェイスの数をクリアする例を示します。

```
hostname# clear ip audit count
```

関連コマンド

コマンド	説明
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show ip audit count	監査ポリシーのシグニチャ一致の数を表示します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

clear ip verify statistics

ユニキャスト RPF 統計情報をクリアするには、特権 EXEC モードで **clear ip verify statistics** コマンドを使用します。ユニキャスト RPF をイネーブルにする方法については、**ip verify reverse-path** コマンドを参照してください。

clear ip verify statistics [**interface** *interface_name*]

構文の説明

interface *interface_name*	ユニキャスト RPF 統計情報をクリアするインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ユニキャスト RPF 統計情報をクリアする例を示します。

```
hostname# clear ip verify statistics
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear ipsec sa

IPSec SA を完全にクリアするには、または指定したパラメータに基づいてクリアするには、特権 EXEC モードで **clear ipsec sa** コマンドを使用します。代替の形式である **clear crypto ipsec sa** も使用できます。

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

構文の説明

counters	（任意）すべてのカウンタをクリアします。
entry	（任意）指定した IPSec ピア、プロトコル、および SPI の IPSec SA をクリアします。
map *map-name*	（任意）指定したクリプト マップの IPSec SA をクリアします。
peer	（任意）指定したピアの IPSec SA をクリアします。
peer-addr	IPSec ピアの IP アドレスを指定します。
protocol	IPSec プロトコル **esp** または **ah** を指定します。
spi	IPSec SPI を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、グローバル コンフィギュレーション モードで、すべての IPSec SA カウンタをクリアする例を示します。

```
hostname# clear ipsec sa counters
hostname#
```

関連コマンド

コマンド	説明
show ipsec sa	指定されたパラメータに基づいて IPSec SA を表示します。
show ipsec stats	IPSec フロー MIB のグローバル IPSec 統計情報を表示します。

clear ipv6 access-list counters

IPv6 アクセス リスト統計情報カウンタをクリアするには、特権 EXEC モードで **clear ipv6 access-list counters** コマンドを使用します。

clear ipv6 access-list *id* **counters**

構文の説明

id	IPv6 アクセス リストの識別子。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IPv6 アクセス リスト 2 の統計情報データをクリアする例を示します。

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

関連コマンド

コマンド	説明
clear configure ipv6	現在のコンフィギュレーションから **ipv6 access-list** コマンドをクリアします。
ipv6 access-list	IPv6 アクセス リストを設定します。
show ipv6 access-list	現在のコンフィギュレーション内の **ipv6 access-list** コマンドを表示します。

clear ipv6 mld traffic

IPv6 Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタをクリアするには、特権 EXEC モードで **clear ipv6 mld traffic** コマンドを使用します。

clear ipv6 mld traffic

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

clear ipv6 mld traffic コマンドを使用すると、すべてのマルチキャスト リスナー検出トラフィック カウンタをリセットできます。

例

次に、IPv6 マルチキャスト リスナー検出のトラフィック カウンタをクリアする例を示します。

```
hostname# clear ipv6 mld traffic
hostname#
```

関連コマンド

コマンド	説明
debug ipv6 mld	マルチキャスト リスナー検出のすべてのデバッグ メッセージを表示します。
show debug ipv6 mld	現在のコンフィギュレーション内の **ipv6** マルチキャスト リスナー検出コマンドを表示します。

clear ipv6 neighbors

IPv6 ネイバー探索キャッシュをクリアするには、特権 EXEC モードで **clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、検出されたすべての IPv6 ネイバーをキャッシュから削除します。スタティック エントリは削除しません。

例

次に、IPv6 ネイバー探索キャッシュのすべてのエントリ（スタティック エントリは除く）を削除する例を示します。

```
hostname# clear ipv6 neighbors
hostname#
```

関連コマンド

コマンド	説明
ipv6 neighbor	IPv6 探索キャッシュ内のスタティック エントリを設定します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、特権 EXEC モードで **clear ipv6 traffic** コマンドを使用します。

clear ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、**show ipv6 traffic** コマンドの出力内のカウンタがリセットされます。

例

次に、IPv6 トラフィック カウンタをリセットする例を示します。**ipv6 traffic** コマンドの出力には、カウンタがリセットされたことが示されています。

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
```

```
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

clear isakmp sa

すべての IKE ランタイム SA データベースを削除するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear isakmp sa** コマンドを使用します。

clear isakmp sa

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**clear isakmp sa** コマンドが、**clear crypto isakmp sa** に変更されました。

例

次に、コンフィギュレーションから IKE ランタイム SA データベースを削除する例を示します。

```
hostname# clear isakmp sa
hostname#
```

関連コマンド

コマンド	説明
clear isakmp	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear local-host

show local-host コマンドを入力することによって表示されるローカル ホストからネットワーク接続を解放するには、特権 EXEC モードで **clear local-host** コマンドを使用します。

clear local-host [*ip_address*] [**all**]

構文の説明

all	（任意）セキュリティ アプライアンスへの接続およびセキュリティ アプライアンスからの接続を含むローカル ホスト状態のホストが作成した接続を消去することを指定します。
ip_address	（任意）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear local-host コマンドは、消去されたホストをライセンス制限から除外します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

注意　ローカル ホストのネットワーク状態を消去すると、ローカル ホストに関連するネットワーク接続と xlate がすべて停止します。

例

次の例では、**clear local-host** コマンドでローカル ホストに関する情報を消去する方法を示します。

```
hostname# clear local-host 10.1.1.15
```

情報がクリアされると、ホストが接続を再確立するまで、何も表示されません。

関連コマンド

コマンド	説明
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ロギング バッファをクリアするには、特権 EXEC モードで **clear logging asdm** コマンドを使用します。

clear logging asdm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear pdm logging** コマンドから **clear asdm log** コマンドに変更されました。

使用上のガイドライン

ASDM システム ログ メッセージは、セキュリティ アプライアンスのシステム ログ メッセージとは別のバッファに格納されます。ASDM ロギング バッファをクリアすると、ASDM システム ログ メッセージだけがクリアされます。セキュリティ アプライアンスのシステム ログ メッセージはクリアされません。ASDM システム ログ メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次に、ASDM ロギング バッファをクリアする例を示します。

```
hostname(config)# clear logging asdm
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ロギング バッファの内容を表示します。

clear logging queue

ログ関連のキューをクリアするには、特権 EXEC モードで **clear logging queue** コマンドを使用します。

clear logging queue [bufferwrap]

構文の説明

bufferwrap	FTP およびフラッシュ ログ バッファをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

例

次に、FTP およびフラッシュ ログ バッファをクリアする例を示します。

```
hostname# clear logging queue bufferwrap
```

関連コマンド

コマンド	説明
logging buffered	ロギング バッファを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリをクリアするには、特権 EXEC モードで **clear mac-address-table** コマンドを使用します。

clear mac-address-table [*interface_name*]

構文の説明

interface_name	（任意）選択したインターフェイスの MAC アドレス テーブル エントリをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ダイナミック MAC アドレス テーブルのエントリをクリアする例を示します。

```
hostname# clear mac-address-table
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory delayed-free-poisoner

delayed free-memory poisoner ツールのキューと統計情報をクリアするには、特権 EXEC モードで **clear memory delayed-free-poisoner** コマンドを使用します。

clear memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドは、delayed free-memory poisoner ツールのキューで保持されているすべてのメモリを検証なしでシステムに戻し、関連する統計情報カウンタをクリアします。

例

次に、delayed free-memory poisoner ツールのキューと統計情報をクリアする例を示します。

```
hostname# clear memory delayed-free-poisoner
```

関連コマンド

コマンド	説明
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキューを検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファをクリアするには、特権 EXEC モードで **clear memory profile** コマンドを使用します。

clear memory profile [peak]

構文の説明

peak	（任意）ピーク メモリ バッファの内容をクリアします。

デフォルト

デフォルトでは、現在「使用されている」プロファイル バッファをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory profile コマンドは、プロファイリング機能によって保持されているメモリ バッファを解放します。したがって、プロファイリングは、クリアされる前に停止している必要があります。

例

次に、プロファイリング機能によって保持されているメモリ バッファをクリアする例を示します。

```
hostname# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。

clear mfib counters

MFIB ルータ パケット カウンタをクリアするには、特権 EXEC モードで **clear mfib counters** コマンドを使用します。

clear mfib counters [*group* [*source*]]

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべての MFIB ルータ パケット カウンタをクリアする例を示します。

```
hostname# clear mfib counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウント データを表示します。

clear module recover

hw-module module recover コマンドで設定された AIP SSM のリカバリ ネットワーク設定をクリアするには、特権 EXEC モードで **clear module recover** コマンドを使用します。

clear module 1 recover

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、AIP SSM のリカバリ設定をクリアする例を示します。

```
hostname# clear module 1 recover
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、AIP SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	AIP SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

clear nac-policy

NAC ポリシーの使用状況の統計情報をリセットするには、グローバル コンフィギュレーション モードで **clear nac-policy** コマンドを使用します。

clear nac-policy [*nac-policy-name***]**

構文の説明

nac-policy-name	（任意）使用状況の統計情報をリセットする NAC ポリシーの名前。

デフォルト

名前を指定しない場合、CLI は、すべての NAC ポリシーに関する使用状況の統計情報をリセットします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次のコマンドでは、framework1 という名前の NAC ポリシーの使用状況の統計情報をリセットしています。

```
hostname(config)# clear nac-policy framework1
```

次のコマンドでは、NAC ポリシーの使用状況の統計情報をすべてリセットしています。

```
hostname(config)# clear nac-policy
```

関連コマンド

コマンド	説明
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

clear nat counters

NAT ポリシー カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear nat counters** コマンドを使用します。

clear nat counters [*src_if* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

構文の説明

dst_ifc	（任意）フィルタリングする宛先インターフェイスを指定します。
dst_ip	（任意）フィルタリングする宛先 IP アドレスを指定します。
dst_mask	（任意）宛先 IP アドレスのマスクを指定します。
src_ifc	（任意）フィルタリングする送信元インターフェイスを指定します。
src_ip	（任意）フィルタリングする送信元 IP アドレスを指定します。
src_mask	（任意）送信元 IP アドレスのマスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0 (4)	このコマンドが導入されました。

例

次に、NAT ポリシー カウンタをクリアする例を示します。

```
hostname(config)# clear nat counters
```

関連コマンド

コマンド	説明
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
nat-control	NAT コンフィギュレーション要件をイネーブルまたはディセーブルにします。
show nat counters	プロトコル スタック カウンタを表示します。

clear ospf

OSPF プロセス情報をクリアするには、特権 EXEC モードで **clear ospf** コマンドを使用します。

clear ospf [*pid*] {**process** | **counters** [**neighbor** [*neighbor-intf*] [*neighbr-id*]]}

構文の説明

counters	OSPF カウンタをクリアします。
neighbor	OSPF ネイバー カウンタをクリアします。
neighbor-intf	（任意）OSPF インターフェイス ルータ指定をクリアします。
neighbr-id	（任意）OSPF 隣接ルータ ID をクリアします。
pid	（任意）OSPF ルーティング プロセスの内部使用の ID パラメータ。有効な値は、1 ～ 65535 です。
process	OSPF ルーティング プロセスをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、コンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドをクリアするには、このコンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。

（注）　**clear configure router ospf** コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドをクリアしません。

例

次に、OSPF プロセス カウンタをクリアする例を示します。

```
hostname# clear ospf process
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべてのグローバル ルータ コマンドをクリアします。

clear pc

PC に保持されている接続情報、xlate 情報、またはローカル ホスト情報をクリアするには、特権 EXEC モードで **clear pc** コマンドを使用します。

clear pc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PC 情報をクリアする例を示します。

```
hostname# clear pc
```

関連コマンド

コマンド	説明
clear pclu	PC 論理更新統計情報をクリアします。

clear pclu

PC 論理更新統計情報をクリアするには、特権 EXEC モードで **clear pclu** コマンドを使用します。

clear pclu

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PC 情報をクリアする例を示します。

```
hostname# clear pclu
```

関連コマンド

コマンド	説明
clear pc	PC に保持されている接続情報、xlate 情報、またはローカル ホスト情報をクリアします。

clear pim counters

PIM トラフィック カウンタをクリアするには、特権 EXEC モードで **clear pim counters** コマンドを使用します。

clear pim counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、トラフィック カウンタだけをクリアします。PIM トポロジ テーブルをクリアするには、**clear pim topology** コマンドを使用します。

例

次に、PIM トラフィック カウンタをクリアする例を示します。

```
hostname# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim topology	PIM トポロジ テーブルをクリアします。
show pim traffic	PIM トラフィック カウンタを表示します。

clear pim reset

リセットによって MRIB 同期を強制するには、特権 EXEC モードで **clear pim reset** コマンドを使用します。

clear pim reset

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トポロジ テーブルのすべての情報がクリアされ、MRIB 接続がリセットされます。このコマンドは、PIM トポロジ テーブルと MRIB データベース間の状態を同期するために使用できます。

例

次に、トポロジ テーブルをクリアし、MRIB 接続をリセットする例を示します。

```
hostname# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim topology

PIM トポロジ テーブルをクリアするには、特権 EXEC モードで **clear pim topology** コマンドを使用します。

clear pim topology [*group*]

構文の説明

group	（任意）トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

オプションの *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートをクリアします。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけがクリアされます。

例

次に、PIM トポロジ テーブルをクリアする例を示します。

```
hostname# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear priority-queue statistics

任意のインターフェイスまたは設定されたすべてのインターフェイスのプライオリティ キュー統計情報カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear priority-queue statistics** コマンドを使用します。

clear priority-queue statistics [*interface-name*]

構文の説明

interface-name	（任意）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティ キュー統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、特権 EXEC モードで **clear priority-queue statistics** コマンドを使用して、「test」という名前のインターフェイスのプライオリティ キュー統計情報を削除する例を示します。

```
hostname# clear priority-queue statistics test
hostname#
```

関連コマンド

コマンド	説明
clear configure priority queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear resource usage

リソース使用状況の統計情報をクリアするには、特権 EXEC モードで **clear resource usage** コマンドを使用します。

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

構文の説明

context *context_name*	（マルチ モードのみ）統計情報をクリアするコンテキスト名を指定します。すべてのコンテキストを対象にする場合は、**all**（デフォルト）を指定します。
resource [**rate**] *resource_name*	特定のリソースの使用状況をクリアします。すべてのリソースを対象にするには、**all**（デフォルト）を指定します。リソース使用状況のレートをクリアする場合は、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM 管理セッション。 • **conns**：1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション インスペクション。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **mac-addresses**：トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチ モードのみ）結合されたコンテキスト統計情報をクリアします。
system	（マルチ モードのみ）システム全体（グローバル）の使用状況の統計情報をクリアします。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** で、これにより、すべてのコンテキストのリソース使用状況がクリアされます。シングル モードの場合、コンテキスト名は無視され、すべてのリソース統計情報がクリアされます。

デフォルトのリソース名は **all** で、これにより、すべてのリソース タイプがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、すべてのコンテキストの、すべてのリソース使用状況の統計情報（システム全体の使用状況の統計情報は除く）をクリアする例を示します。

```
hostname# clear resource usage
```

次に、システム全体の使用状況の統計情報をクリアする例を示します。

```
hostname# clear resource usage system
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

clear route

ダイナミックに学習されたルートをコンフィギュレーションから削除するには、特権 EXEC モードで **clear route** コマンドを使用します。

clear route [*interface_name*]

構文の説明

interface_name	（任意）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ダイナミックに学習されたルートを削除する例を示します。

```
hostname# clear route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの動作データまたは統計情報（存在する場合）をクリアするには、特権 EXEC モードで **clear service-policy** コマンドを使用します。インスペクション エンジンのサービス ポリシーの統計情報をクリアする方法については、**clear service-policy inspect** コマンドを参照してください。

clear service-policy [**global** | **interface** *intf*]

構文の説明

global	（任意）グローバル サービス ポリシーの統計情報をクリアします。
interface *intf*	（任意）特定のインターフェイスのサービス ポリシーの統計情報をクリアします。

デフォルト

デフォルトでは、このコマンドは、すべてのイネーブルなサービス ポリシーのすべての統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**clear service-policy** コマンドの構文例を示します。

```
hostname# clear service-policy outside_security_map interface outside
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	GTP インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
clear service-policy inspect radius-accounting	RADIUS アカウンティング インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

グローバル GTP 統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect gtp** コマンドを使用します。

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

構文の説明

all	すべての GTP PDP コンテキストをクリアします。
apn	（任意）指定した APN に基づいて PDP コンテキストをクリアします。
ap_name	特定のアクセス ポイント名を指定します。
gsn	（任意）GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスである GPRS サポート ノードを指定します。
gtp	（任意）GTP のサービス ポリシーをクリアします。
imsi	（任意）指定した IMSI に基づいて PDP コンテキストをクリアします。
IMSI_value	特定の IMSI を識別する 16 進数値。
interface	（任意）特定のインターフェイスを指定します。
int	情報をクリアするインターフェイスを指定します。
IP_address	統計情報をクリアする IP アドレス。
ms-addr	（任意）指定した MS アドレスに基づいて PDP コンテキストをクリアします。
pdp-context	（任意）パケット データ プロトコル コンテキストを指定します。
requests	（任意）GTP 要求をクリアします。
statistics	（任意）**inspect gtp** コマンドの GTP 統計情報をクリアします。
tid	（任意）指定した TID に基づいて PDP コンテキストをクリアします。
tunnel_ID	特定のトンネルを識別する 16 進数値。
version	（任意）GTP バージョンに基づいて PDP コンテキストをクリアします。
version_num	PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、異なる GSN ノードの 2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークと Mobile Station（MS; モバイル ステーション）ユーザとの間でパケットを転送する場合に必要です。

例

次に、GTP 統計情報をクリアする例を示します。

```
hostname# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションで使用する GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定 GTP マップを表示します。

clear service-policy inspect radius-accounting

RADIUS アカウンティング ユーザをクリアするには、特権 EXEC モードで **clear service-policy inspect radius-accounting** コマンドを使用します。

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

構文の説明

all	すべてのユーザをクリアします。
ip_address	この IP アドレスのユーザをクリアします。
policy_map	このポリシー マップに関連付けられているユーザをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、すべての RADIUS ユーザをクリアする例を示します。

```
hostname# clear service-policy inspect radius-accounting users all
```

clear shun

現在イネーブルであるすべての shun をディセーブルにして、shun 統計情報をクリアするには、特権 EXEC モードで **clear shun** コマンドを使用します。

clear shun [*statistics*]

構文の説明

statistics	（任意）インターフェイス カウンタだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、現在イネーブルになっているすべての shun をディセーブルにして、shun 統計情報をクリアする例を示します。

```
hostname(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。
show shun	回避についての情報を表示します。

clear startup-config errors

メモリからコンフィギュレーション エラー メッセージをクリアするには、特権 EXEC モードで **clear startup-config errors** コマンドを使用します。

clear startup-config errors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示するには、**show startup-config errors** コマンドを使用します。

例

次に、メモリからすべてのコンフィギュレーション エラーをクリアする例を示します。

```
hostname# clear startup-config errors
```

関連コマンド

コマンド	説明
show startup-config errors	セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示します。

clear sunrpc-server active

Sun RPC アプリケーション インスペクションによって開けられたピンホールをクリアするには、特権 EXEC モードで **clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Sun RPC アプリケーション インスペクションによって開けられた、NFS や NIS などのサービス トラフィックがセキュリティ アプライアンスを通過できるようにするピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

例

次に、SunRPC サービス テーブルをクリアする例を示します。

```
hostname# clear sunrpc-server
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスからの Sun リモート プロセッサ コール サービスをクリアします。
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。
show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、特権 EXEC モードで **clear threat detection rate** コマンドを使用して統計情報をクリアできます。

clear threat-detection rate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、レート統計情報をクリアする例を示します。

```
hostname# clear threat-detection rate
```

関連コマンド

コマンド	説明
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection scanning-threat

threat-detection scanning-threat コマンドでスキャンによる脅威の検出をイネーブルにしている場合は、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用して、攻撃者および攻撃対象をクリアします。

clear threat-detection scanning-threat [attacker [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定の IP アドレスをクリアします。
mask	（任意）サブネット マスクを設定します。
attacker	（任意）攻撃者だけをクリアします。
target	（任意）攻撃対象だけをクリアします。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

現在の攻撃者および攻撃対象を表示するには、**show threat-detection scanning-threat** コマンドを使用します。

例

次に、**show threat-detection scanning-threat** コマンドで攻撃対象と攻撃者を表示し、次にすべての攻撃対象をクリアする例を示します。

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
```

```
    192.168.10.9
hostname# clear threat-detection scanning-threat target
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection shun

threat-detection scanning-threat コマンドでスキャンによる脅威の検出をイネーブルにし、ホストへの攻撃を自動的に回避している場合は、特権 EXEC モードで **clear threat-detection shun** コマンドを使用して、現在回避されているホストを解放します。

clear threat-detection shun [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定の IP アドレスの回避を解除します。
mask	（任意）回避されているホストの IP アドレスのサブネット マスクを設定します。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

現在回避されているホストを表示するには、**show threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドで現在回避されているホストを表示し、ホスト 10.1.1.6 を回避状態から解放する例を示します。

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
hostname# clear threat-detection shun 10.1.1.6 255.255.255.255
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection statistics

threat-detection statistics tcp-intercept コマンドで TCP 代行受信の統計情報をイネーブルにしている場合は、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用してこの統計情報をクリアします。

clear threat-detection statistics [tcp-intercept]

構文の説明

tcp-intercept	（任意）TCP 代行受信の統計情報をクリアします。これはデフォルトです。

デフォルト

TCP 代行受信の統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 代行受信の統計情報を表示するには、**show threat-detection statistics top** コマンドを入力します。

例

次に、**show threat-detection statistics top tcp-intercept** コマンドで TCP 代行受信の統計情報を表示し、次にすべての統計情報をクリアする例を示します。

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

```
hostname# clear threat-detection statistics
```

関連コマンド

コマンド	説明
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威の検出の統計情報をイネーブルにします。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、特権 EXEC モードで **clear traffic** コマンドを使用します。

clear traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear traffic コマンドは、**show traffic** コマンドで表示される送信アクティビティと受信アクティビティのカウンタをリセットします。これらのカウンタは、最後に clear traffic コマンドが入力されてから、またはセキュリティ アプライアンスがオンラインになってからの、各インターフェイスを通過したパケット数およびバイト数を示します。また、秒数は、セキュリティ アプライアンスが最後にリブートされてからオンラインである継続時間を示します。

例

次に、**clear traffic** コマンドの例を示します。

```
hostname# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのキャッシュされた認証および認可情報をすべて削除するには、特権 EXEC モードで **clear uauth** コマンドを使用します。

clear uauth [*username*]

構文の説明

username	（任意）削除するユーザ認証情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear uauth コマンドは、1 人のユーザまたはすべてのユーザの AAA 認可および認証のキャッシュを削除します。これにより、これらのユーザは、次回接続を作成するときに、再認証を強制されるようになります。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、セキュリティ アプライアンスではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザが再認証されるようにする例を示します。

```
hostname(config)# clear uauth user
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	**aaa-server** コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
show uauth	現在のユーザ認証および認可情報を表示します。
timeout	アイドル時間の最大継続期間を設定します。

clear url-block block statistics

ブロック バッファ使用状況カウンタをクリアするには、特権 EXEC モードで **clear url-block block statistics** コマンドを使用します。

clear url-block block statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-block block statistics コマンドは、ブロック バッファ使用状況カウンタ（`Current number of packets held (global)` カウンタは除く）をクリアします。

例

次に、URL ブロック統計情報をクリアし、クリア後のカウンタのステータスを表示する例を示します。

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
------------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。

show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド ステートメントを削除するには、特権 EXEC モードで **clear url-cache** コマンドを使用します。

clear url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから **url-cache** 統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティ ニーズを満たす使用状況プロファイルを取得した後に、**| url-cache** コマンドを入力してスループットを向上させます。Websense プロトコル バージョン 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、URL キャッシュ統計情報をクリアする例を示します。

```
hostname# clear url-cache statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。

url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報をクリアするには、特権 EXEC モードで **clear url-server** コマンドを使用します。

clear url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次に、URL サーバの統計情報をクリアする例を示します。

```
hostname# clear url-server statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear wccp

WCCP 情報をリセットするには、特権 EXEC モードで **clear wccp** コマンドを使用します。

clear wccp [**web-cache** | *service_number*]

構文の説明

web-cache	Web キャッシュ サービスを指定します。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、Web キャッシュ サービスの WCCP 情報をリセットする例を示します。

```
hostname# clear wccp web-cache
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear webvpn sso-server statistics

webvpn Single Sign-On（SSO; シングル サインオン）サーバの統計情報をリセットするには、特権 EXEC モードで **clear webvpn sso-server statistics** コマンドを使用します。

clear webvpn sso-server statistics *servername*

構文の説明

servername	無効にする SSO サーバの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

「保留要求」の統計情報はリセットされません。

例

次に、特権 EXEC モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
hostname # clear webvpn sso-server statistics
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear xlate

現在の変換情報および接続情報を消去するには、特権 EXEC モードで **clear xlate** コマンドを使用します。

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*]

構文の説明

global *ip1*[**-***ip2*]	（任意）グローバル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
gport *port1*[**-***port2*]	（任意）グローバル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
interface *if_name*	（任意）アクティブな変換をインターフェイス別に表示します。
local *ip1*[**-***ip2*]	（任意）ローカル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
lport *port1*[**-***port2*]	（任意）ローカル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
netmask *mask*	（任意）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（任意）状態を指定して、アクティブな変換をクリアします。次の 1 つ以上の状態を入力できます。 • **static**：スタティック変換を指定します。 • **portmap**：PAT グローバル変換を指定します。 • **norandomseq**：**norondomseq** 設定での **nat** またはスタティック変換を指定します。 • **identity**：**nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ってください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容をクリアします（「xlate」は変換スロットを意味します）。変換スロットは、キーの変更が行われた後でも存続できます。コンフィギュレーション内で **aaa-server**、**access-list**、**alias**、**global**、**nat**、**route**、または **static** コマンドを追加、変更、または削除した後には、必ず **clear xlate** コマンドを使用します。

xlate は、NAT または PAT セッションについて記述します。これらのセッションは、**detail** オプションを指定した **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックという 2 つのタイプがあります。

スタティック xlate は、**static** コマンドを使用して作成される永続的な xlate です。**clear xlate** コマンドは、スタティック エントリ内のホストをクリアしません。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** コマンドは、スタティック変換ルールを削除しません。コンフィギュレーションから static コマンドを削除しても、スタティック ルールを使用する既存の接続はトラフィックを引き続き転送できます。これらの接続を無効にするには、**clear local-host** コマンドを使用します。

ダイナミック xlate は、**nat** コマンドまたは **global** コマンドを介したトラフィック処理で必要に応じて作成される xlate です。**clear xlate** コマンドを実行すると、ダイナミック xlate および関連付けられた接続が削除されます。また、**clear local-host** コマンドを使用して、xlate および関連付けられた接続を消去することもできます。コンフィギュレーションから **nat** コマンドまたは **global** コマンドを削除した場合、ダイナミック xlate および関連する接続がアクティブのまま残る場合があります。これらの接続を削除するには、**clear xlate** コマンドまたは **clear local-host** コマンドを使用します。

例

次に、現在の変換および接続スロット情報をクリアする例を示します。

```
hostname# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報をクリアします。
clear uauth	キャッシュされたユーザ認証および認可情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。

CHAPTER 8

client access rule コマンド～ crl configure コマンド

client-access-rule

リモートアクセス クライアントのタイプを制限する規則およびセキュリティ アプライアンスを通して IPSec 経由で接続できるバージョンを設定するには、グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

すべてのルールを削除するには、priority 引数だけを指定して **no client-access-rule command** コマンドを使用します。これにより、**client-access-rule none** コマンドを発行して作成されたヌル ルールを含む、設定済みのすべてのルールが削除されます。

クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。ユーザがクライアント アクセス ルールを継承しないようにするには、**client-access-rule none** コマンドを使用します。これにより、すべてのクライアント タイプおよびバージョンが接続できるようになります。

client-access-rule *priority* **{permit | deny} type** *type* **version** *version* **| none**

no client-access-rule *priority* [**{permit | deny} type** *type* **version** *version*]

構文の説明

deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、セキュリティ アプライアンスはそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** で表示される値と完全に一致する必要があります。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** で表示される値と完全に一致する必要があります。

デフォルト

デフォルトでは、アクセス ルールはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次の注意に従ってルールを作成します。

- ルールを定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、セキュリティ アプライアンスは接続を拒否します。つまり、拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。許可ルールを定義しないと、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントの両方について、タイプおよびバージョンが **show vpn-sessiondb remote** での表示の内容と完全に一致する必要があります。
- * 文字はワイルドカードであり、各ルールで複数回使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x ソフトウェアを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールを作成します。
- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプとバージョンを送信しないクライアントに対して n/a を使用できます。

例

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、ソフトウェア バージョン 4.1 を実行している VPN クライアントを許可する一方で、すべての VPN 3002 ハードウェア クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client（CTL プロバイダー）

証明書信頼リスト プロバイダーへの接続が許可されるクライアントを指定するか、またはクライアント認証用のユーザ名とパスワードを指定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

構文の説明

encrypted	パスワードの暗号化を指定します。
interface *if_name*	接続が許可されるインターフェイスを指定します。
ipv4_addr	クライアントの IP アドレスを指定します。
username *user_name*	クライアント認証用のユーザ名を指定します。
password *password*	クライアント認証用のパスワードを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL プロバイダー コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダーへの接続を許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを設定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。複数のコマンドを発行して、複数のクライアントを定義できます。ユーザ名とパスワードは、CallManager クラスタ用の CCM 管理者のユーザ名およびパスワードと一致する必要があります。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client（TLS プロキシ）

トラストポイント、キー ペア、および暗号スイートを設定するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

構文の説明

cipher-suite *cipher_suite*	暗号スイートを指定します。オプションには、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、および null-sha1 が含まれます。
issuer *ca_tp_name*	クライアントのダイナミック証明書を発行するローカル CA トラストポイントを指定します。
keypair *key_label*	クライアントのダイナミック証明書で使用する RSA キー ペアを指定します。
ldc	ローカル ダイナミック証明書の発行者またはキー ペアを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

TLS プロキシで TLS クライアント ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを制御するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。これには、暗号スイートのコンフィギュレーションか、ローカル ダイナミック証明書の発行者またはキー ペアの設定が含まれます。クライアントのダイナミック証明書を発行するローカル CA は、**crypto ca trustpoint** コマンドで定義され、トラストポイントでは **proxy-ldc-issuer** を設定するか、デフォルトのローカル CA サーバ（LOCAL-CA-SERVER）を使用する必要があります。

キー ペア値は、**crypto key generate** コマンドを使用して生成されている必要があります。

クライアント プロキシ（サーバに対して TLS クライアントとして機能するプロキシ）の場合、ユーザ定義の暗号スイートによって、デフォルトの暗号スイート、または **ssl encryption** コマンドで定義された暗号スイートが置き換えられます。このコマンドでは、2 つの TLS セッション間で異なる暗号を設定できます。CallManager サーバでは、AES 暗号を使用する必要があります。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client-firewall

IKE トンネルのネゴシエーション時に セキュリティ アプライアンス が VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を使用します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを使用します。**client-firewall none** コマンドを発行して作成したヌル ポリシーを含め、すべての設定済みファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがそれらのファイアウォール ポリシーを継承しないようにするには、**client-firewall none** コマンドを使用します。

client-firewall none

client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

（注） ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

構文の説明

acl-in <*acl*>	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out <*acl*>	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。セキュリティ アプライアンスは、ファイアウォールが実行されていることを確認するためのチェックを行います。「Are You There?」と表示され、応答がない場合は、セキュリティ アプライアンスによりトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。

cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアント ファイアウォール ポリシーのソースとしてプッシュされるポリシーを指定します。
custom	カスタム ファイアウォール タイプを指定します。
description <*string*>	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーをヌル値に設定します。これによりファイアウォール ポリシーが禁止されます。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**zonelabs-integrity** ファイアウォール タイプが追加されました。

使用上のガイドライン

設定できるのは、このコマンドの 1 つのインスタンスのみです。

例

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

Cisco Unified Presence Server（CUPS）の TLS プロキシを設定する場合、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS プロキシ コンフィギュレーション モードで **client trust-point** コマンドを使用します。プロキシ トラストポイント証明書を削除するには、このコマンドの **no** 形式を使用します。

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint*]

構文の説明

proxy_trustpoint	**crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

client trust-point コマンドは、セキュリティ アプライアンスが TLS クライアントの役割を果たしている場合に、TLS ハンドシェイク時にセキュリティ アプライアンスが使用するトラストポイントと関連証明書を指定します。証明書は、セキュリティ アプライアンス が所有している必要があります（ID 証明書）。

証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**client trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

例

次に、client trust-point コマンドを使用して、TLS サーバでの TLS ハンドシェイクでトラストポイント「ent_y_proxy」の使用を指定する例を示します。ハンドシェイクは、エンティティ Y から開始され、TLS サーバが常駐するエンティティ X に対して行われるとします。ASA は、エンティティ Y の TLS プロキシとして機能します。

```
hostname(config-tlsp)# client trust-point ent_y_proxy
```

関連コマンド

コマンド	説明
client（TLS プロキシ）	TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。
server trust-point	セキュリティ アプライアンスが TLS サーバの役割を果たす場合、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

client-types（クリプト CA トラスト ポイント）

ユーザ接続に関連付けられた証明書の検証にこのトラストポイントを使用できるクライアント接続タイプを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **client-types command** コマンドを使用します。指定した接続にトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[no] client-types {ssl | ipsec}

構文の説明

ipsec	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを IPSec 接続の検証に使用できることを指定します。
ssl	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド履歴

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

同じ CA 証明書に関連付けられているトラストポイントが複数ある場合、特定のクライアント タイプに設定できるのは 1 つのトラストポイントだけです。ただし、1 つのトラストポイントを 1 つのクライアント タイプに設定し、別のトラストポイントを別のクライアント タイプに設定することができます。

同じ CA 証明書に関連付けられているトラストポイントがあり、これがすでに 1 つのクライアント タイプに設定されている場合は、この同じクライアント タイプ設定に新しいトラストポイントを設定することはできません。このコマンドの no 形式を使用して設定をクリアして、トラストポイントがいずれのクライアント検証にも使用できないようにすることができます。

リモート アクセス VPN では、配置の要件に応じて、Secure Sockets Layer（SSL）VPN、IP Security（IPSec; IP セキュリティ）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを IPsec トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

client-update

すべてのトンネル グループまたは特定のトンネル グループで、アクティブなすべてのリモート VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンス用のクライアント更新を発行するには、特権 EXEC モードで **client-update** コマンドを使用します。

クライアント更新のパラメータをグローバル レベル（VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンスを含む）で設定および変更するには、グローバル コンフィギュレーション モードで **client-update** コマンドを使用します。

VPN ソフトウェア クライアントとハードウェア クライアント用のクライアント更新トンネル グループ IPSec 属性パラメータを設定および変更するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **client-update** コマンドを使用します。

リビジョン番号のリストにあるソフトウェア バージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェア バージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。

クライアント更新をディセーブルにするには、このコマンドの **no** 形式を使用します。

グローバル コンフィギュレーション モードのコマンドは、次のとおりです。

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

トンネル グループ IPSec 属性モードのコマンドは、次のとおりです。

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

特権 EXEC モードのコマンドは、次のとおりです。

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

構文の説明

all	（特権 EXEC モードでのみ使用可能）すべてのトンネル グループのすべてのアクティブ リモート クライアントにアクションを適用します。キーワード **all** をこのコマンドの **no** 形式で使用することはできません。
component {**asdm** | **image**}	Auto Update クライアントとして設定されているセキュリティ アプライアンスのソフトウェア コンポーネント。
device-id *dev_string*	固有のストリングで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じストリングを指定します。最大で 63 文字です。
enable	（グローバル コンフィギュレーション モードでのみ使用可能）リモート クライアントのソフトウェア更新をイネーブルにします。
family *family_name*	デバイス ファミリで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じデバイス ファミリを指定します。これは、asa、pix、または最大 7 文字のテキスト ストリングです。

rev-nums *rev-nums*	（特権 EXEC モードでは使用不可）このクライアントのソフトウェア イメージまたはファームウェア イメージを指定します。Windows、WIN9X、WinNT、および vpn3002 の各クライアントは、任意の順番で 4 つまで、カンマで区切って指定できます。セキュリティ アプライアンスの場合は、1 つしか指定できません。ストリングの最大長は 127 文字です。
tunnel-group	（特権 EXEC モードでのみ使用可能）リモート クライアント更新の有効なトンネル グループの名前を指定します。
type *type*	（特権 EXEC モードでは使用不可）クライアント更新を通知するために、リモート PC のオペレーティング システム、または Auto Update クライアントとして設定されているセキュリティ アプライアンスのタイプを指定します。このリストは、次の内容で構成されます。 • asa5505：Cisco 5505 適応型セキュリティ アプライアンス • asa5510：Cisco 5510 適応型セキュリティ アプライアンス • asa5520：Cisco 5520 適応型セキュリティ アプライアンス • asa5540：Cisco 適応型セキュリティ アプライアンス • linux：Linux クライアント • mac：MAC OS X クライアント • pix-515：Cisco PIX 515 Firewall • pix-515e：Cisco PIX 515E Firewall • pix-525：Cisco PIX 525 Firewall • pix-535：Cisco PIX 535 Firewall • Windows：Windows ベースのすべてのプラットフォーム • WIN9X：Windows 95、Windows 98、および Windows ME プラットフォーム • WinNT：Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム • vpn3002：VPN 3002 ハードウェア クライアント • 最大 15 文字のテキスト ストリング
url *url-string*	（特権 EXEC モードでは使用不可）ソフトウェア イメージまたはファームウェア イメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。ストリングの最大長は 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。
7.2(1)	Auto Update サーバとして設定されたセキュリティ アプライアンスをサポートするために、**component**、**device-id**、および **family** キーワードとその引数が追加されました。

使用上のガイドライン　トンネル グループ ipsec 属性コンフィギュレーション モードでは、この属性を IPSec リモート アクセス トンネル グループ タイプのみに適用できます。

client-update コマンドを使用すると、更新のイネーブル化、更新の適用先となるクライアントのタイプとリビジョン番号の指定、更新の取得元となる URL または IP アドレスの指定を実行できます。また、Windows クライアントの場合は、VPN クライアント バージョンを更新する必要があることを任意でユーザに通知できます。Windows クライアントに対しては、更新を実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザに対しては、更新は通知なしで自動的に実行されます。クライアントのタイプが別のセキュリティ アプライアンスである場合は、このセキュリティ アプライアンスが Auto Update サーバとして機能します。

クライアント更新メカニズムを設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント更新をイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

ステップ 2　グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用する、クライアント更新用のパラメータを設定します。つまり、クライアントのタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。Auto Update クライアントの場合は、ソフトウェア コンポーネント（ASDM またはブート イメージ）を指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。このコマンドは、セキュリティ アプライアンス全体にわたって、指定したタイプのすべてのクライアントに適用されるクライアント更新パラメータを設定します。次に例を示します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

VPN 3002 ハードウェア クライアントのトンネル グループを設定する場合の図については、「例」の項を参照してください。

（注）　すべての Windows クライアントと Auto Update クライアントで、URL のプレフィックスとして、「http://」または「https://」プロトコルを使用する必要があります。VPN3002 ハードウェア クライアントに対しては、代わりにプロトコル「tftp://」を指定する必要があります。

また、Windows クライアントと VPN3002 ハードウェア クライアントでは、特定のタイプのすべてのクライアントではなく、個々のトンネル グループだけのクライアント更新を設定することもできます（ステップ 3 を参照）。

（注）　URL の末尾にアプリケーション名を含めることで（例：**https://support/updates/vpnclient.exe**）、アプリケーションを自動的に起動するようにブラウザを設定できます。

ステップ 3　クライアント更新をイネーブルにした後に、特定の ipsec-ra トンネル グループの一連のクライアント更新パラメータを定義できます。これを行うには、トンネル グループ ipsec 属性モードで、トンネル グループの名前とタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。たとえば、すべての Windows クライアント用のクライアント更新を発行する必要はありません。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

VPN 3002 ハードウェア クライアントのトンネル グループを設定する場合の図については、「例」の項を参照してください。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

ステップ 4　任意で、古い Windows クライアントを使用しているアクティブ ユーザに、VPN クライアントの更新が必要であることを知らせる通知を送信できます。これらのユーザに対しては、ポップアップ ウィンドウが表示されます。ユーザはこのポップアップ ウィンドウからブラウザを起動して、URL で指定されているサイトから、更新されたソフトウェアをダウンロードできます。このメッセージで設定可能な部分は URL だけです （ステップ 2 または 3 を参照）。アクティブでないユーザは、次回ログイン時に通知メッセージを受信します。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信するか、または特定のトンネル グループのクライアントに送信できます。たとえば、すべてのトンネル グループのすべてのアクティブ クライアントに通知する場合は、特権 EXEC モードで次のコマンドを入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。また、ユーザは通知メッセージを受信しません。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

（注）　クライアント更新のタイプを **windows**（Windows ベースのすべてのプラットフォーム）に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント更新タイプを入力する必要が生じた場合は、まずこのコマンドの **no** 形式で windows クライアント タイプを削除してから、新しい client-update コマンドを使用して新しいクライアント タイプを指定します。

例

次に、グローバル コンフィギュレーション モードで、すべてのトンネル グループのすべてのアクティブ リモート クライアントに対してクライアント更新をイネーブルにする例を示します。

```
hostname(config)# client-update enable
hostname#
```

次の例は、Windows（win9x、winnt、または windows）だけに適用されます。グローバル コンフィギュレーション モードで、Windows ベースのすべてのクライアントのクライアント更新パラメータを設定します。リビジョン番号 4.7、および更新を取得する URL（https://support/updates）を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.7
hostname(config)#
```

次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec 属性コンフィギュレーション モードに入ると、IPSec リモート アクセス トンネル グループ「salesgrp」用のクライアント アップデート パラメータが設定されます。リビジョン番号 4.7 を指定し、TFTP プロトコルを使用して、更新されたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
hostname(config-tunnel-ipsec)#
```

次に、Auto Update クライアントとして設定されている Cisco 5520 適応型セキュリティ アプライアンスであるクライアントのクライアント更新を発行する例を示します。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

次に、特権 EXEC モードで、クライアント ソフトウェアの更新が必要なトンネル グループ「remotegrp」内の、接続中のすべてのリモート クライアントにクライアント更新通知を送信する例を示します。他のグループのクライアントは、更新通知を受け取りません。

```
hostname# client-update remotegrp
hostname#
```

関連コマンド

コマンド	説明
clear configure client-update	クライアントアップデート コンフィギュレーション全体をクリアします。
show running-config client-update	現在のクライアント アップデート コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

clock set

セキュリティ アプライアンスのクロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

構文の説明

day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
hh:*mm*:*ss*	時、分、秒を 24 時間形式で設定します。たとえば、午後 8 時 54 分は **20:54:00** のように設定します。
month	月を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clock コンフィギュレーション コマンドを入力していない場合、**clock set** コマンドのデフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。ただし、**clock timezone** コマンドを使用して時間帯を設定した後に **clock set** コマンドを入力した場合は、UTC ではなく、新しい時間帯に応じた時間を入力します。同様に、**clock set** コマンドの後に **clock summer-time** コマンドを入力した場合、時間は夏時間に調整されます。**clock summer-time** コマンドの後に **clock set** コマンドを入力した場合は、夏時間の正しい時間を入力します。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドの新しい時刻を設定する必要があります。

例

次に、時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定し、MDT の現在の時間を 2004 年 7 月 27 日の午後 1 時 15 分に設定する 例を示します。

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

次に、クロックを UTC 時間帯で 2004 年 7 月 27 日の 8 時 15 分に設定し、次に時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定する例を示します。終了時間（MDT の 1 時 15 分）は前の例と同じです。

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

関連コマンド

コマンド	説明
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在時刻を表示します。

clock summer-time

セキュリティ アプライアンスの時間の表示に夏時間の日付範囲を設定するには、グローバル コンフィギュレーション モードで **clock summer-time** コマンドを使用します。夏時間の日付をディセーブルにするには、このコマンドの **no** 形式を使用します。

clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]]

構文の説明

date	夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このキーワードを使用する場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
hh:mm	時間と分を 24 時間形式で設定します。
month	月をストリングで設定します。**date** コマンドでは、たとえば、標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
offset	（任意）夏時間の時間を変更する分数を設定します。デフォルト値は 60 分です。
recurring	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このキーワードを使用すると、定期的な日付範囲を設定できるため、毎年変更する必要がありません。日付を指定しない場合、セキュリティ アプライアンスが米国で使用するデフォルトの日付範囲は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時となります。
week	（任意）週を 1 ～ 4 の整数で指定するか、**first** や **last** の語で指定します。たとえば、日付が 5 週目に当たる場合は、**last** を指定します。
weekday	（任意）**Monday**、**Tuesday**、**Wednesday** などの曜日を指定します。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。
zone	太平洋夏時間の時間帯をストリング（**PDT** など）で指定します。このコマンドで設定した日付範囲に従ってセキュリティ アプライアンスが夏時間を表示する場合、時間帯はここで設定した値に変更されます。基本の時間帯を UTC 以外の時間帯に設定するには、**clock timezone** を参照してください。

デフォルト

デフォルトのオフセットは 60 分です

定期的な日付範囲のデフォルト値は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	変更後の定期的な日付範囲のデフォルト値は、3 月の第二日曜日の午前 2 時～ 11 月の第一日曜日の午前 2 時。

使用上のガイドライン

南半球の場合、セキュリティ アプライアンスは、開始月が終了月よりも後に来る（10 月～ 3 月など）ことを受け入れます。

例

次に、オーストラリアの夏時間の日付範囲を設定する例を示します。

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

国によっては、夏時間が特定の日付に開始されます。次の例では、夏時間は 2004 年 4 月 1 日午前 3 時に始まり、2004 年 10 月 1 日午前 4 時に終わるように設定されています。

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

clock timezone

セキュリティ アプライアンスのクロックの時間帯を設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを使用します。時間帯をデフォルトの UTC に戻すには、このコマンドの **no** 形式を使用します。**clock set** コマンド、または NTP サーバから生成された時間は、時間を UTC で設定します。このコマンドを使用して、時間帯を UTC のオフセットとして設定する必要があります。

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

構文の説明

zone	太平洋標準時間の時間帯をストリング（**PST** など）で指定します。
[**-**]*hours*	UTC からのオフセットの時間数を設定します。たとえば、PST は **-8** 時間です。
minutes	（任意）UTC からのオフセットの分数を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

夏時間を設定するには、**clock summer-time** コマンドを参照してください。

例

次に、時間帯を太平洋標準時間（UTC から -8 時間）に設定する例を示します。

```
hostname(config)# clock timezone PST -8
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。

コマンド	説明
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

cluster-ctl-file

フラッシュ メモリに格納されている既存の CTL ファイルから、すでに作成されているトラストポイントを使用するには、CTL ファイル コンフィギュレーション モードで **cluster-ctl-file** コマンドを使用します。CTL ファイルのコンフィギュレーションを削除して、新しい CTL ファイルを作成できるようにするには、このコマンドの **no** 形式を使用します。

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

構文の説明

filename_path	ディスクまたはフラッシュ メモリに格納されている CTL ファイルのパスおよびファイル名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL ファイル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

このコマンドが設定されている場合、電話プロキシは、フラッシュ メモリに格納されている CTL ファイルを解析し、その CTL ファイルからのトラストポイントをインストールし、フラッシュのそのファイルを使用して新しい CTL ファイルを作成します。

例

次に、**cluster-ctl-file** コマンドを使用して、フラッシュ メモリに格納されている CTL ファイルを解析し、そのファイルからトラストポイントをインストールする例を示します。

```
hostname(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。

コマンド	説明
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

cluster encryption

仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化をイネーブルにするには、VPN ロード バランシング コンフィギュレーション モードで **cluster encryption** コマンドを使用します。暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

cluster encryption

no cluster encryption

（注） VPN ロード バランシングには、アクティブな 3DES または AES ライセンスが必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

暗号化は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化のオンとオフを切り替えます。

cluster encryption コマンドを設定する前に、まず **vpn load-balancing** コマンドを使用して VPN ロード バランシング モードを開始する必要があります。また、クラスタの暗号化をイネーブルにする前に、**cluster key** コマンドを使用してクラスタ共有秘密キーを設定する必要があります。

（注）　暗号化を使用する場合は、最初にコマンド **isakmp enable** *inside* を設定する必要があります。ここで、*inside* は、ロード バランシングの内部インターフェイスを示します。ロード バランシングの内部インターフェイスで ISAKMP がイネーブルでない場合は、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

例

次に、仮想ロード バランシング クラスタの暗号化をイネーブルにする **cluster encryption** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
cluster key	クラスタの共有秘密キーを指定します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster ip address

仮想ロード バランシング クラスタの IP アドレスを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster ip address** コマンドを使用します。IP アドレスの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

構文の説明

ip-address	仮想ロード バランシング クラスタに割り当てる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最初に、**vpn load-balancing** コマンドを使用して VPN ロード バランシング コンフィギュレーション モードを開始し、仮想クラスタ IP アドレスが指すインターフェイスを設定する必要があります。

このクラスタ IP アドレスは、仮想クラスタを設定するインターフェイスと同じサブネット上にある必要があります。

このコマンドの **no** 形式では、任意の *ip-address* 値を指定した場合、**no cluster ip address** コマンドを実行するには、その値が既存のクラスタの IP アドレスと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの IP アドレスを 209.165.202.224 に設定する **cluster ip address** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

```
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
interface	デバイスのインターフェイスを設定します。
nameif	インターフェイスに名前を割り当てます。
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster key

仮想ロード バランシング クラスタ上で交換される IPSec サイトツーサイト トンネルの共有秘密を設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster key** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

cluster key *shared-secret*

no cluster key [*shared-secret*]

構文の説明

shared-secret	VPN ロード バランシング クラスタの共有秘密を定義する 3 ～ 17 文字のストリング。ストリングに特殊文字を含めることはできますが、スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。クラスタの暗号化には、**cluster key** コマンドで定義された秘密も使用されます。

共有秘密を設定するには、クラスタの暗号化をイネーブルにする前に **cluster key** コマンドを使用する必要があります。

このコマンドの **no cluster key** 形式で *shared-secret* の値を指定した場合、共有秘密の値は既存のコンフィギュレーションと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの共有秘密を 123456789 に設定する **cluster key** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
```

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

cluster-mode

クラスタのセキュリティ モードを指定するには、電話プロキシ コンフィギュレーション モードで **cluster-mode** コマンドを使用します。クラスタのセキュリティ モードをデフォルト モードに設定するには、このコマンドの **no** 形式を使用します。

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

構文の説明

mixed	電話プロキシ機能の設定時に、クラスタ モードを混合モードとすることを指定します。
nonsecure	電話プロキシ機能の設定時に、クラスタ モードを非セキュア モードとすることを指定します。

デフォルト

デフォルトのクラスタ モードは非セキュアです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

電話プロキシを混合モード クラスタ（セキュア モードと非セキュア モードの両方）で実行するように設定する場合は、一部の電話が認証または暗号化モードで設定されている場合に備えて LDC 発行元も設定する必要があります。

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

例

次に、**cluster-mode** コマンドを使用して、電話プロキシを混合（IP 電話がセキュア モードと非セキュア モードの両方で動作）に設定する例を示します。

```
hostname(config-phone-proxy)# cluster-mode mixed
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

cluster port

仮想ロード バランシング クラスタの UDP ポートを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster port** コマンドを使用します。ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster port *port*

no cluster port [*port*]

構文の説明

port	仮想ロード バランシング クラスタに割り当てる UDP ポート。

デフォルト

デフォルトのクラスタ ポートは 9023 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。

任意の有効な UDP ポート番号を指定できます。範囲は 1 ～ 65535 です。

このコマンドの **no cluster port** 形式で *port* の値を指定した場合、指定したポート番号は既存の設定済みポート番号と一致する必要があります。

例

次に、仮想ロード バランシング クラスタの UDP ポートを 9023 に設定する **cluster port address** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
```

```
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

command-alias

コマンドのエイリアスを作成するには、グローバル コンフィギュレーション モードで **command-alias** コマンドを使用します。エイリアスを削除するには、このコマンドの **no** 形式を使用します。コマンド エイリアスを入力すると、元のコマンドが呼び出されます。たとえば、コマンド エイリアスを作成して、長いコマンドのショートカットにすることができます。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

構文の説明

mode	**exec**（ユーザ EXEC モードおよび特権 EXEC モード）、**configure**、**interface** など、コマンド エイリアスを作成するコマンド モードを指定します。
command_alias	既存のコマンドに付ける新しい名前を指定します。
original_command	コマンド エイリアスを作成する既存のコマンドまたはキーワードがあるコマンドを指定します。

デフォルト

デフォルトでは、次のユーザ EXEC モード エイリアスが設定されます。

help の場合は **h**

logout の場合は **lo**

ping の場合は **p**

show の場合は **s**

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

任意のコマンドの最初の部分のエイリアスを作成し、さらに通常どおり追加のキーワードと引数を入力できます。

CLI ヘルプを使用する場合、コマンド エイリアスはアスタリスク（*）で示され、次の形式で表示されます。

```
*command-alias=original-command
```

たとえば、**lo** コマンド エイリアスは、次のように、「lo」で始まる他の特権 EXEC モードのコマンドとともに表示されます。

```
hostname# lo?
*lo=logout login  logout
```

同じエイリアスをさまざまなモードで使用できます。たとえば、次のように、特権 EXEC モードおよびコンフィギュレーション モードで、「happy」を異なる複数のコマンドのエイリアスとして使用できます。

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

コマンドだけを表示し、エイリアスを省略するには、入力行の先頭にスペースを入力します。また、コマンド エイリアスを回避するには、コマンドを入力する前にスペースを使用します。次の例では、happy? コマンドの前にスペースがあるため、エイリアスの happy が表示されていません。コマンドを使用します。

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

コマンドの場合と同様に、CLI ヘルプを使用して、コマンド エイリアスの後に続く引数およびキーワードを表示できます。

完全なコマンド エイリアスを入力する必要があります。短縮されたエイリアスは使用できません。次の例では、パーサーはエイリアスの happy を示すコマンドの hap を認識しません。

```
hostname# hap
% Ambiguous command: "hap"
```

例

次に、**copy running-config startup-config** コマンドに対して「**save**」という名前のコマンド エイリアスを作成する例を示します。

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

関連コマンド

コマンド	説明
clear configure command-alias	デフォルト以外のすべてのコマンド エイリアスをクリアします。
show running-config command-alias	デフォルト以外の設定済みのコマンド エイリアスをすべて表示します。

command-queue

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

command-queue *limit*

no command-queue *limit*

構文の説明

limit	キューに入れるコマンドの最大数（1 ～ 2147483647）を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

MGCP コマンド キューのデフォルトは 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには **command-queue** コマンドを使用します。許可されている値の範囲は、1 ～ 4294967295 です。デフォルトは 200 です。制限値に達した状態で新しいコマンドが着信すると、最も長時間キューに入っているコマンドが削除されます。

例

次に、MGCP コマンドのキューを 150 コマンドに制限する例を示します。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。
timeout	アイドル タイムアウトを設定します。タイムアウト後に、MGCP メディア接続または MGCP PAT xlate 接続が閉じられます。

compatible rfc1583

RFC 1583 に従った集約ルート コストの計算に使用した方式に戻すには、ルータ コンフィギュレーション モードで **compatible rfc1583** コマンドを使用します。RFC 1583 互換性をディセーブルにするには、このコマンドの **no** 形式を使用します。

compatible rfc1583

no compatible rfc1583

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。

例

次に、RFC 1583 互換のルート集約コスト計算をディセーブルにする例を示します。

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

compression

SVC 接続および WebVPN 接続で圧縮をイネーブルにするには、グローバル コンフィギュレーション モードで **compression** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

構文の説明

all	使用可能なすべての圧縮技術をイネーブルにすることを指定します。
svc	SVC 接続に対する圧縮を指定します。
http-comp	WebVPN 接続に対する圧縮を指定します。

デフォルト

デフォルトは、*all* です。使用可能なすべての圧縮技術がイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

SVC 接続の場合、グローバル コンフィギュレーション モードで設定した **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定した **svc compression** コマンドは上書きされます。

たとえば、グループ ポリシー webvpn モードで特定のグループに対する **svc compression** コマンドを入力し、次にグローバル コンフィギュレーション モードで **no compression** コマンドを入力した場合、そのグループに対して設定した **svc compression** コマンドの設定は上書きされます。

逆に、グローバル コンフィギュレーション モードで **compression** コマンドを使用して圧縮をオンに戻した場合は、グループ設定が有効となり、圧縮動作は最終的にグループ設定によって決定されます。

no compression コマンドを使用して圧縮をディセーブルにした場合、新しい接続だけが影響を受けます。アクティブな接続は影響を受けません。

例

次に、SVC 接続で圧縮をオンにする例を示します。

```
hostname(config)# compression svc
```

次に、SVC 接続および WebVPN 接続で圧縮をディセーブルにする例を示します。

```
hostname(config)# no compression svc http-comp
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションに関する情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc compression	特定のグループまたはユーザに対して SVC 接続を介する HTTP データの圧縮をイネーブルにします。

config-register

次回セキュリティ アプライアンスをリロードするときに使用されるコンフィギュレーション レジスタ値を設定するには、グローバル コンフィギュレーション モードで **config-register** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、ASA 5500 適応型セキュリティ アプライアンスでのみサポートされています。コンフィギュレーション レジスタ値は、ブート元のイメージおよび他のブート パラメータを決定します。

config-register *hex_value*

no config-register

構文の説明

hex_value	コンフィギュレーション レジスタ値を 0x0 ～ 0xFFFFFFFF の 16 進数値に設定します。この数は 32 ビットを表し、各 16 進文字は 4 ビットを表します。それぞれのビットが異なる特性を制御します。ただし、ビット 32 ～ 20 は将来の使用のために予約されており、ユーザが設定できないか、または現在セキュリティ アプライアンスで使用されていません。したがって、これらのビットを表す 3 つの文字は常に 0 に設定されているため、無視できます。関連するビットは、5 桁の 16 進文字（0x*nnnnn*）で表されます。 文字の前の 0 は含める必要はありません。後続の 0 は含める必要があります。たとえば、0x2001 は 0x02001 と同じですが、0x10000 の 0 はすべて必要です。関連するビットに使用できる値の詳細については、表 8-1 を参照してください。

デフォルト

デフォルト値は 0x1 であり、ローカル イメージおよびスタートアップ コンフィギュレーションからブートします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

5 つの文字には、右から左への方向で 0 ～ 4 の番号が付けられます。これは、16 進数および 2 進数の場合には標準的です。各文字に対して 1 つの値を選択したり、必要に応じて値を組み合わせて一致させたりすることができます。たとえば、文字番号 3 に対して 0 または 2 を選択できます。他の値との競合が生じる場合、一部の値が優先されます。たとえば、セキュリティ アプライアンスを TFTP サーバとローカル イメージの両方からブートするように設定する 0x2011 を設定した場合、セキュリティ アプ

ライアンスは TFTP サーバからブートします。この値は、TFTP のブートが失敗した場合、セキュリティ アプライアンスが直接 ROMMON でブートすることも定めているため、デフォルト イメージからブートすることを指定したアクションは無視されます。

0 の値は、他に指定されていなければ、アクションを実行しないことを意味します。

表 8-1 に、各 16 進文字に関連付けられたアクションを示します。各文字に対して 1 つの値を選択します。

表 8-1　コンフィギュレーション レジスタ値

プレフィックス	16 進数文字番号 4、3、2、1、および 0				
0x	**0**	**0**	**0**[1]	**0**[2]	**0**[2]
	1 起動中に 10 秒の ROMMON のカウントダウンをディセーブルにします。通常は、カウントダウン中に Escape キーを押して ROMMON を開始できます。	**2** TFTP サーバからブートするようにセキュリティ アプライアンスを設定している場合、ブートが失敗すると、この値は直接 ROMMON でブートします。		**1** ROMMON ブート パラメータ（存在する場合は、**boot system tftp** コマンドと同じ）で指定されたように TFTP サーバ イメージからブートします。この値は、文字 1 に設定された値よりも優先されます。	**1** 最初の **boot system** *local_flash* コマンドで指定されたイメージをブートします。そのイメージがロードされない場合、セキュリティ アプライアンスは、正常にブートするまで後続の **boot system** コマンドで指定された各イメージのブートを試行します。
					3、5、7、9 特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。 イメージが正常にブートしない場合、セキュリティ アプライアンスは他の **boot system** コマンド イメージに戻ることを試行しません（この点が値 1 と値 3 の使用における違いです）。ただし、セキュリティ アプライアンスには、ブートが失敗した場合に内部フラッシュ メモリのルート ディレクトリ内で検出された任意のイメージからブートを試行するフェールセーフ機能があります。フェールセーフ機能を有効にしない場合は、ルート以外のディレクトリにイメージを保存します。
				4[3] スタートアップ コンフィギュレーションを無視してデフォルトのコンフィギュレーションをロードします。	**2、4、6、8** ROMMON で、**boot** コマンドを引数なしで入力した場合、セキュリティ アプライアンスは特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。この値はイメージを自動的にブートしません。
				5 上記の両方のアクションを実行します。	

1. 将来的な使用のために予約されています。

2. 文字番号 0 および 1 が、イメージを自動的にブートするように設定されていない場合、セキュリティ アプライアンスは直接 ROMMON でブートします。
3. **service password-recovery** コマンドを使用してパスワード回復をディセーブルにした場合は、スタートアップ コンフィギュレーションを無視するようにコンフィギュレーション レジスタを設定することはできません。

コンフィギュレーション レジスタ値はスタンバイ ユニットに複製されませんが、アクティブ ユニットにコンフィギュレーション レジスタを設定すると、次の警告が表示されます。

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

confreg コマンドを使用して、コンフィギュレーション レジスタ値を ROMMON で設定することもできます。

例

次に、デフォルト イメージからブートするようにコンフィギュレーション レジスタを設定する例を示します。

```
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
service password-recovery	パスワードの回復をイネーブルまたはディセーブルにします。

configure factory-default

コンフィギュレーションを出荷時のデフォルトに戻すには、グローバル コンフィギュレーション モードで **configure factory-default** コマンドを使用します。出荷時のデフォルトのコンフィギュレーションは、シスコが新しいセキュリティ アプライアンスに適用しているコンフィギュレーションです。このコマンドは、PIX 525 および PIX 535 のセキュリティ アプライアンスを除くすべてのプラットフォームでサポートされています。

configure factory-default [*ip_address* [*mask*]]

構文の説明

ip_address	デフォルトのアドレス 192.168.1.1 を使用する代わりに、管理インターフェイスまたは内部インターフェイスの IP アドレスを設定します。各モデルで設定されるインターフェイスの詳細については、「使用上のガイドライン」を参照してください。
mask	インターフェイスのサブネット マスクを設定します。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスに適したマスクを使用します。

デフォルト

デフォルトの IP アドレスとマスクは 192.168.1.1 および 255.255.255.0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	出荷時のデフォルトのコンフィギュレーションが ASA 5505 適応型セキュリティ アプライアンスに追加されました。

使用上のガイドライン

PIX 515/515E および ASA 5510 以上のセキュリティ アプライアンスでは、出荷時のデフォルトのコンフィギュレーションによって、管理用のインターフェイスが自動的に設定されるため、ASDM を使用してそのインターフェイスに接続し、残りの設定を実行できます。ASA 5505 適応型セキュリティ アプライアンスでは、出荷時のデフォルトのコンフィギュレーションによって、セキュリティ アプライアンスをネットワークですぐに使用できるように、インターフェイスと NAT が自動的に設定されます。

このコマンドは、ルーテッド ファイアウォール モードでのみ使用可能です。トランスペアレント モードはインターフェイスの IP アドレスをサポートしていません。インターフェイス IP アドレスの設定は、このコマンドが行うアクションの 1 つです。また、このコマンドはシングル コンテキスト モードでのみ使用できます。コンフィギュレーションをクリアされたセキュリティ アプライアンスには、このコマンドを使用して自動的に設定される定義済みのコンテキストはありません。

このコマンドは現在の実行コンフィギュレーションをクリアしてから、複数のコマンドを設定します。

configure factory-default コマンドで IP アドレスを設定した場合、**http** コマンドは、ユーザが指定したサブネットを使用します。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

出荷時のデフォルトのコンフィギュレーションに戻した後に、**write memory** コマンドを使用してこのコンフィギュレーションを内部フラッシュ メモリに保存します。**write memory** コマンドは、前に **boot config** コマンドで別の場所を設定している場合でも、その設定をクリアしたときにパスもクリアされているので、スタートアップ コンフィギュレーション用のデフォルトの場所に実行コンフィギュレーションを保存します。

（注）　このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** を使用すると、外部フラッシュ メモリ カードのイメージを含む特定のイメージからブートできます。出荷時のコンフィギュレーションに戻した後、次回セキュリティ アプライアンスをリロードすると、セキュリティ アプライアンスは、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、はブートしません。

完全なコンフィギュレーションに有用な追加の設定を行うには、**setup** コマンドを参照してください。

ASA 5505 適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5505 適応型セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- イーサネット 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定していない場合、VLAN 1 の IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- イーサネット 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は、DHCP を使用してその IP アドレスを取得します。
- デフォルトのルートも DHCP から取得されます。
- すべての内部 IP アドレスが、外部にアクセスするときにインターフェイス PAT によって変換されます。
- デフォルトでは、内部ユーザはアクセス リストを使用して外部にアクセスでき、外部ユーザは内部にアクセスできません。
- セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、VLAN 1 インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取ります。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
```

```
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以上の適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5510 以上の適応型セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- 管理用 Management 0/0 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。
- セキュリティ アプライアンスでは DHCP サーバがイネーブルにされているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E セキュリティ アプライアンスのコンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。

- セキュリティ アプライアンスでは DHCP サーバがイネーブルにされているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

例

次に、コンフィギュレーションを出荷時のデフォルトにリセットし、IP アドレス 10.1.1.1 をインターフェイスに割り当て、次に新しいコンフィギュレーションをスタートアップ コンフィギュレーションとして保存する例を示します。

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

関連コマンド

コマンド	説明
boot system	ブート元のソフトウェア イメージを設定します。
clear configure	実行コンフィギュレーションをクリアします。
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
setup	セキュリティ アプライアンスの基本設定を設定するよう要求します。
show running-config	実行コンフィギュレーションを表示します。

configure http

HTTP(S) サーバから実行コンフィギュレーションにコンフィギュレーション ファイルをマージするには、グローバル コンフィギュレーション モードで **configure http** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

configure http[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

構文の説明

:password	（任意）HTTP(S) 認証の場合、パスワードを指定します。
:*port*	（任意）ポートを指定します。HTTP の場合、デフォルトは 80 です。HTTPS の場合、デフォルトは 443 です。
@	（任意）名前とパスワードの両方またはいずれかを入力する場合は、サーバの IP アドレスの前にアットマーク（@）を付けます。
filename	コンフィギュレーション ファイル名を指定します。
http[**s**]	HTTP または HTTPS を指定します。
path	（任意）ファイル名へのパスを指定します。
server	サーバの IP アドレスまたは名前を指定します。IPv6 サーバ アドレスでポートを指定する場合は、IP アドレス内のコロンがポート番号の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスとポートを次のように入力します。 `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（任意）HTTP(S) 認証の場合、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルト ポートは 80 です。HTTPS の場合、デフォルト ポートは 443 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィ

ギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

このコマンドは、**copy http running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure http** コマンドはコンテキスト内で使用するための代替です。

例

次に、コンフィギュレーション ファイルを HTTPS サーバから実行コンフィギュレーションにコピーする例を示します。

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力されたコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure memory

スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure memory** コマンドを使用します。

configure memory

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

コンフィギュレーションをマージしない場合は、セキュリティ アプライアンスを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、**configure memory** コマンドを入力して新しいコンフィギュレーションをロードできます。

このコマンドは、**copy startup-config running-config** コマンドと同じです。

マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、**config-url** コマンドで指定した場所にあります。

例

次に、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーする例を示します。

```
hostname(config)# configure memory
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力されたコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure net

TFTP サーバのコンフィギュレーション ファイルを実行コンフィギュレーションにマージするには、グローバル コンフィギュレーション モードで **configure net** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

configure net [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 このコマンドでファイル名を指定し、**tftp-server** コマンドで名前を指定する場合、セキュリティ アプライアンスは **tftp-server** コマンド ファイル名をディレクトリとして扱い、**configure net** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。IPv6 サーバ アドレスの場合、IP アドレス内のコロンがファイル名の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスを次のように入力します。 [fe80::2e0:b6ff:fe01:3b7a] デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。マージによって実行コンフィギュレーションに存在しているコマンドが削除されることはありません。そのコマンドは新しいコンフィギュレーションでは設定されないだけです。

このコマンドは、**copy tftp running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure net** コマンドはコンテキスト内で使用するための代替です。

例

次に、**tftp-server** コマンドにサーバとファイル名を設定してから、**configure net** コマンドを使用してサーバを上書きする例を示します。同じファイル名が使用されています。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

次に、サーバおよびファイル名を上書きする例を示します。ファイル名へのデフォルト パスは /tftpboot/configs/config1 です。ファイル名をスラッシュ（/）で始めない場合、パスの /tftpboot/ 部分がデフォルトで含まれます。このパスを上書きし、ファイルも tftpboot にある場合は、tftpboot パスを **configure net** コマンドに含めます。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

次に、サーバだけを **tftp-server** コマンドに設定する例を示します。**configure net** コマンドはファイル名だけを指定します。

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

configure terminal

実行コンフィギュレーションをコマンドラインで設定するには、特権 EXEC モードで **configure terminal** コマンドを使用します。このコマンドは、コンフィギュレーションを変更するコマンドを入力できるグローバル コンフィギュレーション モードを開始します。

configure terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、グローバル コンフィギュレーション モードを開始する例を示します。

```
hostname# configure terminal
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。

config-url

システムがコンテキスト コンフィギュレーションをダウンロードする URL を指定するには、コンテキスト コンフィギュレーション モードで **config-url** コマンドを使用します。

config-url *url*

構文の説明

url　コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL 構文を参照してください。

- **disk0:**/[*path*/]*filename*

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。

- **disk1:**/[*path*/]*filename*

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。

- **flash:**/[*path*/]*filename*

  この URL は内部フラッシュ メモリを示します。

- **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type には次のキーワードのいずれかを指定できます。

  - **ap**：ASCII 受動モード
  - **an**：ASCII 通常モード
  - **ip**：（デフォルト）バイナリ受動モード
  - **in**：バイナリ通常モード

- **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

- **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*]

  サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コンテキスト URL を追加すると、システムはただちにコンテキストをロードし、実行中になります。

（注） **config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。セキュリティ アプライアンスは、コンテキスト コンフィギュレーションをロードする前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、セキュリティ アプライアンスはただちにコンテキスト コンフィギュレーションをロードします。インターフェイスを示すコマンドがコンテキストに含まれている場合、それらのコマンドは失敗します。

ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。

管理コンテキスト ファイルは、内部フラッシュ メモリに保存する必要があります。

HTTP または HTTPS サーバからコンテキスト コンフィギュレーションをダウンロードした場合、**copy running-config startup-config** コマンドを使用してこれらのサーバに変更内容を戻して保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

システムは、サーバが利用できない、またはファイルがまだ存在しないためにコンテキスト コンフィギュレーション ファイルを取得できない場合、コマンドライン インターフェイスですぐに設定できるブランクのコンテキストを作成します。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。

例

次に、管理コンテキストに「administrator」を設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
```

```
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

console timeout

セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **console timeout** コマンドを使用します ディセーブルにするには、このコマンドの **no** 形式を使用します。

console timeout *number*

no console timeout [*number*]

構文の説明

number	コンソール セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。

デフォルト

デフォルトのタイムアウトは 0 であり、コンソール セッションがタイムアウトしないことを示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

console timeout コマンドは、セキュリティ アプライアンスへの認証済みのすべてのイネーブル モード ユーザ セッションまたはコンフィギュレーション モード ユーザ セッションにタイムアウト値を設定します。**console timeout** コマンドによって、Telnet タイムアウトや SSH タイムアウトが変更されることはありません。これらのアクセス方式では、それぞれ独自のタイムアウト値が保持されています。

no console timeout コマンドは、コンソール タイムアウト値をデフォルトのタイムアウトである 0 にリセットします。この値は、コンソールがタイムアウトしないことを意味します。

例

次に、コンソール タイムアウトを 15 分に設定する例を示します。

```
hostname(config)# console timeout 15
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。

コマンド	説明
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

content-length

HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **content-length** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのインスペクションに合格しなかったときに実行するアクションを指定します。
allow	メッセージを許可します。
bytes	バイト数を指定します。許容される範囲は、**min** オプションでは 1 ～ 65535、**max** オプションでは 1 ～ 50000000 です。
drop	接続を閉じます。
log	（任意）syslog を生成します。
max	（任意）許容される内容の最大長を指定します。
min	（任意）許容される内容の最小長を指定します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。

デフォルト

デフォルトでは、このコマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

content-length コマンドをイネーブルにすると、セキュリティ アプライアンスは、設定された範囲内のメッセージだけを許可し、範囲外の場合は指定されたアクションを実行します。セキュリティ アプライアンスに TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

例

次に、HTTP トラフィックを 100 バイト以上 2000 バイト以下のメッセージに制限する例を示します。メッセージがこの範囲外の場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

context

システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **context** コマンドを使用します。コンテキストを削除するには、このコマンドの **no** 形式を使用します。コンテキスト コンフィギュレーション モードでは、コンテキストで使用できる、コンフィギュレーション ファイルの URL とインターフェイスを指定できます。

context *name*

no context *name* [**noconfirm**]

構文の説明

name	名前を最大 32 文字のストリングで設定します。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。
noconfirm	（任意）確認を求めるプロンプトを表示せずにコンテキストを削除します。このオプションは自動スクリプトで役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

管理コンテキストがない場合（たとえば、コンフィギュレーションをクリアした場合）、追加する最初のコンテキストは管理コンテキストである必要があります。管理コンテキストを追加するには、**admin-context** コマンドを参照してください。管理コンテキストを指定した後、**context** コマンドを入力して管理コンテキストを設定します。

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストはこのコマンドの **no** 形式を使用して削除することはできません。**clear configure context** コマンドを使用してすべてのコンテキストを削除した場合にのみ削除できます。

例

次に、管理コンテキストに「administrator」を設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースの間を切り替えます。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
show context	コンテキスト情報を表示します。

copy

ファイルをある場所から別の場所にコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

copy [**/noconfirm** | **/pcap**] {*url* | **running-config** | **startup-config**}
{**running-config** | **startup-config** | *url*}

構文の説明

/noconfirm	確認のプロンプトを出さないでファイルをコピーします。
/pcap	事前に設定した TFTP サーバのデフォルトを指定します。デフォルトの TFTP サーバを設定する場合は、**tftp-server** コマンドを参照してください。
running-config	メモリに格納されている実行コンフィギュレーションを指定します。

startup-config	フラッシュ メモリに格納されているスタートアップ コンフィギュレーションを指定します。シングル モードのスタートアップ コンフィギュレーション、またはマルチ コンテキスト モードのシステムのスタートアップ コンフィギュレーションは、フラッシュ メモリ内の非表示のファイルです。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。たとえば、**config-url** コマンドで HTTP サーバを指定し、**copy startup-config running-config** コマンドを入力した場合、セキュリティ アプライアンスは管理コンテキスト インターフェイスを使用して、HTTP サーバからスタートアップ コンフィギュレーションをコピーします。

url

コピー元のファイルまたはコピー先のファイルを指定します。コピー元 URL とコピー先 URL のすべての組み合わせが許可されているわけではありません。たとえば、あるリモート サーバから別のリモート サーバにコピーすることはできません。このコマンドは、ローカルの場所とリモートの場所との間でファイルをコピーするために使用します。コンテキスト内では、コンテキスト インターフェイスを使用して、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションを TFTP サーバまたは FTP サーバにコピーできますが、サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコピーすることはできません。他のオプションについては、**startup-config** キーワードを参照してください。TFTP サーバから実行コンテキスト コンフィギュレーションにダウンロードするには、**configure net** コマンドを使用します。

次の URL 構文を使用します。

- **cache:**/[*path*/]*filename*]

  このオプションは、ファイル システム内のキャッシュ メモリを示します。
- **capture:**/[*path*/]*filename*]

  このオプションは、キャプチャ バッファ内の出力を示します。
- **disk0:**/[*path*/]*filename*]

  このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。
- **disk1:**/[*path*/]*filename*]

  このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、外部フラッシュ メモリ カードを示します。
- **flash:**/[*path*/]*filename*]

  このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。
- **smb:**/[*path*/]*filename*]

  このオプションは、UNIX サーバ上のローカル ファイル システムを示します。サーバ メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク オペレーティング システムで使用されます。
- **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type には次のキーワードのいずれかを指定できます。
  - **ap**：ASCII 受動モード
  - **an**：ASCII 通常モード
  - **ip**：（デフォルト）バイナリ受動モード
  - **in**：バイナリ通常モード
- **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*]
- **system:**/[*path*/]*filename*]

  このオプションは、ファイル システム内のシステム メモリを示します。
- **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*]

  サーバ アドレスへのルートを上書きする場合は、**nameif interface** コマンドを使用してインターフェイス名を指定します。

  パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DNS 名のサポートが追加されました。
8.0(2)	**smb:** URL オプションが追加されました。

使用上のガイドライン

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2 つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

例

次に、システム実行スペースでファイルをディスクから TFTP サーバにコピーする例を示します。

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

次に、ファイルをディスク上のある場所からディスク上の別の場所にコピーする例を示します。宛先ファイルの名前は、コピー元のファイルの名前にすることも、別の名前にすることもできます。

```
hostname(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

次に、ASDM ファイルを TFTP サーバから内部フラッシュ メモリにコピーする例を示します。

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

次に、コンテキスト内の実行コンフィギュレーションを TFTP サーバにコピーする例を示します。

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy コマンドでは、IP アドレス（上の例の場合）だけでなく、DNS 名も指定できます。

```
hostname(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

関連コマンド

コマンド	説明
configure net	ファイルを TFTP サーバから実行コンフィギュレーションにコピーします。
copy capture	キャプチャ ファイルを TFTP サーバにコピーします。
tftp-server	デフォルトの TFTP サーバを設定します。

コマンド	説明
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

copy capture

キャプチャ ファイルをサーバにコピーするには、特権 EXEC モードで **copy capture** コマンドを使用します。

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name/*]*buffer_name url*

構文の説明

/noconfirm	確認のプロンプトを出さないでファイルをコピーします。
/pcap	パケット キャプチャを raw データとしてコピーします。
buffer_name	キャプチャを識別するための一意な名前。
context_name/	セキュリティ コンテキストで定義されたパケット キャプチャをコピーします。
url	パケット キャプチャ ファイルのコピー先を指定します。次の URL 構文を参照してください。 • **disk0:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用でき、内部フラッシュ カードを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用でき、外部フラッシュ カードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。 • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**：ASCII 受動モード – **an**：ASCII 通常モード – **ip**：（デフォルト）バイナリ受動モード – **in**：バイナリ通常モード • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、フル パスを指定せずに **copy capture** コマンドを入力した場合に表示されるプロンプトの例を示します。

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

次のようにフル パスを指定できます。

```
hostname(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

TFTP サーバをすでに設定している場合は、次のようにファイルの位置や名前を省略できます。

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

cpu profile activate

CPU のプロファイル コレクションに関する情報を表示するには、特権 EXEC モードで **cpu profile activate** コマンドを使用します。

cpu profile activate *n-samples*

構文の説明

n-samples	サンプル数 n を保存するためのメモリを割り当てます。値は 1 ～ 100000 で、デフォルトは 1000 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show cpu profile コマンドと、**cpu profile activate** コマンドを併用することで、CPU の問題の修復を支援するために TAC が収集および使用できる情報を表示できます。**show cpu profile** コマンドによって表示される情報は 16 進数です。

例

次の例では、プロファイラが稼働し、5000 個のサンプルの格納が命令されます。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

結果を確認するには、**show cpu profile** コマンドを使用します。

（注）　**cpu profile activate** コマンドの実行中に **show cpu profile** を実行すると、進捗が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

完了すると、**show cpu profile** コマンドの出力に結果が表示されます。この情報をコピーし、デコードする TAC に提供します。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000 samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d 002198af
0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show cpu profile	TAC で使用する CPU のプロファイルのアクティベーションに関する情報を表示します。

crashinfo console disable

フラッシュへのクラッシュの書き込みを読み取り、書き込み、設定するには、グローバル コンフィギュレーション モードで **crashinfo console disable** コマンドを使用します。

crashinfo console disable

no crashinfo console disable

構文の説明

disable	クラッシュが発生した場合にコンソール出力を抑制します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、コンソールへの crashinfo の出力を抑制できます。crashinfo には、デバイスに接続しているすべてのユーザに表示するのは適切でない機密情報が含まれている場合があります。このコマンドとともに、crashinfo がフラッシュに書き込まれていることも確認する必要があります。これはデバイスのリブート後に確認できます。このコマンドは、crashinfo および checkheaps の出力に影響を与えます。この出力はフラッシュに保存され、トラブルシューティングに十分に役立ちます。

例

```
hostname(config)# crashinfo console disable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。

コマンド	説明
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

crashinfo force

セキュリティ アプライアンスを強制的にクラッシュさせるには、特権 EXEC モードで **crashinfo force** コマンドを使用します。

crashinfo force [**page-fault** | **watchdog**]

構文の説明

page-fault	（任意）ページ フォールトを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。
watchdog	（任意）ウォッチドッグを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュを、**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュと区別できません。これは、これらのコマンドによって実際にクラッシュが発生しているためです。セキュリティ アプライアンスは、クラッシュのダンプが完了するとリロードします。

注意　実働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはセキュリティ アプライアンスをクラッシュさせて、強制的にリロードを実行します。

例

次に、**crashinfo force page-fault** コマンドを入力したときに表示される警告の例を示します。

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

キーボードの Return キーまたは Enter キーを押して復帰改行を入力するか、**Y** キーまたは **y** キーを押すと、セキュリティ アプライアンスがクラッシュしてリロードが実行されます。これらの応答は、確認済みとして解釈されます。その他の文字はすべて **no** と解釈され、セキュリティ アプライアンスはコマンドライン プロンプトに戻ります。

関連コマンド

clear crashinfo	クラッシュ情報ファイルの内容をクリアします。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo save disable

フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにするには、グローバル コンフィギュレーション モードで **crashinfo save** コマンドを使用します。フラッシュ メモリへのクラッシュ情報の書き込みを許可し、デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

crashinfo save disable

no crashinfo save disable

構文の説明

このコマンドには、デフォルトの引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	**crashinfo save enable** コマンドは廃止され、有効なオプションではなくなりました。代わりに、**no crashinfo save disable** コマンドを使用します。

使用上のガイドライン

クラッシュ情報は、まずフラッシュ メモリに書き込まれ、次にコンソールに書き込まれます。

（注） セキュリティ アプライアンスが起動中にクラッシュした場合、クラッシュ情報ファイルは保存されません。セキュリティ アプライアンスは、完全に初期化され、動作を開始した後に、クラッシュ情報をフラッシュ メモリに保存できます。

フラッシュ メモリへのクラッシュ情報の保存をもう一度イネーブルにするには、**no crashinfo save disable** コマンドを使用します。

例

```
hostname(config)# crashinfo save disable
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容をクリアします。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。

crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

フラッシュ メモリのファイルにクラッシュ情報を保存するセキュリティ アプライアンスの機能をテストするには、特権 EXEC モードで **crashinfo test** コマンドを使用します。

crashinfo test

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

（注）　**crashinfo test** コマンドを入力してもセキュリティ アプライアンスはクラッシュしません。

例

次に、クラッシュ情報ファイル テストの出力例を示します。

```
hostname# crashinfo test
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crl

CRL コンフィギュレーション オプションを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl** コマンドを使用します。

crl {**required** | **optional** | **nocheck**}

構文の説明

required	ピア証明書の検証に必要な CRL が使用可能である必要があります。
optional	必須の CRL が使用できない場合にも、セキュリティ アプライアンスはピア証明書を受け入れることができます。
nocheck	CRL チェックを実行しないようセキュリティ アプライアンスに指示します。

デフォルト

デフォルト値は **nocheck** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。次の **revocation-check** コマンドに置き換わりました。 • **crl optional** は **revocation-check crl none** に置き換えられました。 • **crl required** は **revocation-check crl** に置き換えられました。 • **crl nocheck** は **revocation-check none** に置き換えられました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、ピア証明書がトラストポイント central に対して検証されるのに CRL を必要とする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードを開始します。
crl configure	CRL コンフィギュレーション モードを開始します。

crl configure

CRL コンフィギュレーション モードを開始するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl configure** コマンドを使用します。

crl configure

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central 内で crl コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

CHAPTER 9

crypto ca authenticate コマンド～ customization コマンド

crypto ca authenticate

トラストポイントに関連付けられている CA 証明書をインストールおよび認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。CA 証明書を削除するには、このコマンドの **no** 形式を使用します。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

no crypto ca authenticate *trustpoint*

構文の説明

fingerprint	セキュリティ アプライアンスが CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが指定されている場合、セキュリティ アプライアンスは、そのフィンガープリントを、CA 証明書の計算されたフィンガープリントと比較して、2 つの値が一致した場合にだけその証明書を受け入れます。フィンガープリントがない場合、セキュリティ アプライアンスは計算されたフィンガープリントを表示し、証明書を受け入れるかどうかを尋ねます。
hexvalue	フィンガープリントの 16 進値を指定します。
nointeractive	Device Manager 専用の非対話形式モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、セキュリティ アプライアンスは確認せずに証明書を受け入れます。
trustpoint	CA 証明書を取得するトラストポイントを指定します。名前の最大長は 128 文字です。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。そうでない場合、セキュリティ アプライアンスは、ユーザに Base-64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、CA 証明書を要求するセキュリティ アプライアンスの例を示します。CA は証明書を送信し、セキュリティ アプライアンスは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。セキュリティ アプライアンスの管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。セキュリティ アプライアンスによって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

次に、トラストポイント tp9 が端末ベース（手動）の登録用に設定される例を示します。この場合、セキュリティ アプライアンスは、管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、セキュリティ アプライアンスは、管理者に証明書を保持することを確認するように要求します。

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca enroll	CA への登録を開始します。
crypto ca import certificate	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。
crypto ca trustpoint	指定したトラストポイントに対してトラストポイント サブモードを開始します。

crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを使用します。

crypto ca certificate chain *trustpoint*

構文の説明

trustpoint	証明書チェーンを設定するトラストポイントを指定します。

デフォルト

このコマンドには、デフォルト値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central の CA 証明書チェーン サブモードを開始する例を示します。

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

crypto ca certificate map

CA 証明書マップ モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca configuration map** コマンドを使用します。このコマンドを実行すると、CA 証明書マップ モードが開始されます。証明書マッピング ルールの優先順位付けされたリストを管理するには、このコマンドのグループを使用します。マッピング ルールの順序はシーケンス番号によって決まります。クリプト CA コンフィギュレーション マップ ルールを削除するには、このコマンドの **no** 形式を使用します。

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

構文の説明

map-name	certificate-to-group マップの名前を指定します。
sequence-number	作成する証明書マップ ルールの番号を指定します。指定できる範囲は 1 ～ 65535 です。トンネル グループを証明書マップ ルールにマッピングする tunnel-group-map を作成するときに、この番号を使用できます。

デフォルト

sequence-number のデフォルトの動作や値はありません。

map-name のデフォルトの値は、DefaultCertificateMap です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2	*map-name* キーワードが追加されました。

使用上のガイドライン

このコマンドを発行すると、セキュリティ アプライアンスは CA 証明書マップ コンフィギュレーション モードになります。このモードでは、証明書の発行者名およびサブジェクト Distinguished Name（DN; 認定者名）に基づいてルールを設定できます。これらのルールの一般的な形式は次のとおりです。

DN match-criteria match-value

DN は、*subject-name* または *issuer-name* のいずれかです。DN は、ITU-T X.509 標準で定義されています。証明書フィールドのリストについては、「関連コマンド」を参照してください。

match-criteria は、次の表現または演算子で構成されます。

attr *tag*	比較を Common Name（CN; 一般名）などの特定の DN 属性に制限します。
co	記載内容
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現は大文字と小文字が区別されません。

例

次に、example-map というマップ名とシーケンス番号 1（ルール番号 1）で CA 証明書マップ モードを開始し、subject-name という Common Name（CN; 一般名）属性が Example1 と一致する必要があることを指定する例を示します。

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name attr cn eq Example1
hostname(ca-certificate-map)#
```

次に、example-map というマップ名とシーケンス番号 1 で CA 証明書マップ モードを開始し、subject-name 内に値 cisco が含まれることを指定する例を示します。

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

関連コマンド

コマンド	説明
issuer-name	ルール エントリが IPSec ピア証明書の発行者 DN に適用されることを指定します。
subject-name（クリプト CA 証明書マップ）	ルール エントリが IPSec ピア証明書のサブジェクト DN に適用されることを指定します。
tunnel-group-map enable	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

crypto ca crl request

指定したトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求するには、クリプト CA トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint*

構文の説明

trustpoint	トラストポイントを指定します。文字数は最大で 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、central という名前のトラストポイントに基づいて CRL を要求する例を示します。

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。

crypto ca enroll

CA との登録プロセスを開始するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。このコマンドが正常に実行されるには、トラストポイントが正しく設定されている必要があります。

crypto ca enroll *trustpoint* [**noconfirm**]

構文の説明

noconfirm	（任意）すべてのプロンプトを表示しないようにします。要求される場合がある登録オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または他の非対話形式で使用するためのものです。
trustpoint	登録するトラストポイントの名前を指定します。文字数は最大で 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、セキュリティ アプライアンスはただちに CLI プロンプトを表示し、コンソールへのステータス メッセージを非同期的に表示します。トラストポイントが手動登録用に設定されている場合、セキュリティ アプライアンスは Base-64 エンコード PKCS10 証明書要求をコンソールに書き込んでから、CLI プロンプトを表示します。

このコマンドは、参照されるトラストポイントの設定された状態に応じて、異なる対話形式プロンプトを生成します。

例

次に、SCEP 登録を使用して、トラストポイント tp1 でアイデンティティ証明書を登録する例を示します。セキュリティ アプライアンスは、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
```

```
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

次のコマンドは、CA 証明書の手動登録を示しています。

```
hostname(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。
crypto ca trustpoint	指定したトラストポイントに対してトラストポイント サブモードを開始します。

crypto ca export

セキュリティ アプライアンスのトラストポイント コンフィギュレーションを、関連付けられているすべてのキーおよび証明書とともに PKCS12 形式でエクスポートするには、またはデバイスのアイデンティティ証明書を PEM 形式でエクスポートするには、グローバル コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

crypto ca export *trustpoint* **identify-certificate**

構文の説明

identify-certificate	指定したトラストポイントに関連付けられている登録済み証明書をコンソールに表示することを指定します。
trustpoint	証明書が表示されるトラストポイントの名前を指定します。トラストポイント名の最大文字数は 128 文字です。

デフォルト

このコマンドには、デフォルト値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(2)	このコマンドは、PEM 形式での証明書のエクスポートに対応するために変更されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。PEM データまたは PKCS12 データはコンソールに書き込まれます。

Web ブラウザでは、パスワードベースの対称キーで保護された付属の公開キー証明書とともに秘密キーを格納するために PKCS12 形式を使用しています。セキュリティ デバイスは、トラストポイントに関連付けられている証明書とキーを Base-64 エンコード PKCS12 形式でエクスポートします この機能を使用して、証明書とキーをセキュリティ デバイス間で移動できます。

証明書の PEM エンコーディングは、PEM ヘッダーで囲まれた X.509 証明書の Base-64 エンコーディングです。これは、セキュリティ デバイス間で証明書をテキストベースで転送するための標準的な方法を提供します。セキュリティ デバイスがクライアントとして機能している場合、PEM エンコーディングは、SSL/TLS プロトコル プロキシを利用する *proxy-ldc-issuer* 証明書のエクスポートに使用できます。

例

次に、トラストポイント 222 の PEM 形式の証明書をコンソール表示としてエクスポートする例を示します。

```
hostname (config)# crypto ca export 222 identity-certificate

Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。
crypto ca trustpoint	指定したトラストポイントのトラストポイント コンフィギュレーション モードを開始します。

crypto ca import

手動登録要求への応答で CA から受信した証明書をインストールしたり、PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートしたりするには、グローバル コンフィギュレーション モードで **crypto ca import** コマンドを使用します。セキュリティ アプライアンスは、ユーザに Base-64 形式で端末にテキストを貼り付けるように要求します。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

構文の説明

trustpoint	インポート アクションを関連付けるトラストポイントを指定します。文字数は最大で 128 です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアにはトラストポイントと同じ名前が割り当てられます。
certificate	トラストポイントによって示される CA から証明書をインポートするようセキュリティ アプライアンスに指示します
pkcs12	PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするようセキュリティ アプライアンスに指示します。
passphrase	PKCS12 データの復号化に使用するパスフレーズを指定します。
nointeractive	（任意）非対話形式モードを使用して証明書をインポートします。すべてのプロンプトを表示しないようにします。このオプションは、スクリプト、ASDM、または対話が必要ないその他の場合に使用するオプションです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
```

```
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
hostname (config)#
```

次に、PKCS12 データをトラストポイント central に手動でインポートする例を示します。

```
hostname (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca export	トラストポイントの証明書とキー ペアを PKCS12 形式でエクスポートします。
crypto ca authenticate	トラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントに対してトラストポイント サブモードを開始します。

crypto ca server

セキュリティ アプライアンス上のローカル CA サーバを設定および管理するには、グローバル コンフィギュレーション モードで **crypto ca server** コマンドを使用して設定 ca サーバ コンフィギュレーション モードを開始し、CA コンフィギュレーション コマンドにアクセスします。設定されているローカル CA サーバをセキュリティ アプライアンスから削除するには、このコマンドの **no** 形式を使用します。

crypto ca server

no crypto ca server

デフォルト

認証局サーバは、セキュリティ アプライアンス上でイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス上にローカル CA は 1 つしか存在できません。

crypto ca server コマンドは CA サーバを設定しますが、イネーブルにはしません。ローカル CA をイネーブルにするには、設定 ca サーバ モードで **shutdown** コマンドの **no** 形式を使用します。

no shutdown コマンドで CA サーバをアクティブにすると、CA および LOCAL-CA-SERVER というトラストポイントの RSA キー ペアが確立されて自己署名証明書が保持されます。この新しく生成された自己署名証明書には、「デジタル署名」、「crl 署名」および「証明書の署名」のキー使用設定が常に設定されています。

注意　**no crypto ca server** コマンドは、ローカル CA サーバの現在の状態に関係なく、設定済みのローカル CA サーバ、その RSA キー ペア、および関連付けられているトラストポイントを削除します。

例

次に、このコマンドを使用して設定 ca サーバ コンフィギュレーション モードを開始し、このモードで使用可能なローカル CA サーバ コマンドをリストするために疑問符を使用する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
```

```
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

次に、設定済みでイネーブルになっている CA サーバをセキュリティ アプライアンスから削除するために、設定 ca サーバ モードで **crypto ca server** コマンドの **no** 形式を使用する例を示します。

```
hostname(config-ca-server)#no crypto ca server

Certificate server 'remove server' event has been queued for processing.
hostname(config)#
```

関連コマンド

コマンド	説明
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server	設定されている CA サーバのステータスおよびパラメータを表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。

crypto ca server crl issue

Certificate Revocation List（CRL; 証明書失効リスト）の発行を強制的に行うには、特権 EXEC モードで **crypto ca server crl issue** コマンドを使用します。

crypto ca server crl issue

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは失われた CRL の回復に使われますが、ほとんど使用されることはありません。通常、CRL は失効時に既存の CRL に再署名することで自動的に再発行されます。**crypto ca server crl issue** コマンドは、証明書データベースに基づいて CRL を再生成します。また、このコマンドを使用するのは、証明書データベースの内容に基づいて CRL を再生成する必要がある場合だけです。

例

次に、ローカル CA サーバによる CRL の発行を強制的に行う例を示します。

```
hostname(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA によって発行される証明書に含める証明書失効リスト配布ポイントを指定します。

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ユーザがローカル CA を設定および管理できるようにします。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

crypto ca server revoke

ローカル Certificate Authority（CA; 認証局）サーバによって発行された証明書を証明書データベースと CRL で失効としてマークするには、特権 EXEC モードで **crypto ca server revoke** コマンドを使用します。

crypto ca server revoke *cert-serial-no*

構文の説明

cert-serial-no	失効させる証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス上のローカル CA によって発行された特定の証明書を失効させるには、そのセキュリティ アプライアンスで **crypto ca server revoke** コマンドを入力します。証明書は、このコマンドによって CA サーバの証明書データベースと CRL に失効としてマークされると失効します。失効させる証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書が失効した後に、CRL が自動的に再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書を失効させる例を示します。

```
hostname(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked.A new CRL has been issued.

hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server unrevoke	ローカル CA サーバによって発行され、すでに失効している証明書の失効を取り消します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server unrevoke

ローカル CA サーバによって発行され、すでに失効している証明書の失効を取り消すには、特権 EXEC モードで **crypto ca server unrevoke** コマンドを使用します。

crypto ca server unrevoke *cert-serial-no*

構文の説明

cert-serial-no	失効を取り消す証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス上のローカル CA によって発行され、すでに失効している証明書の失効を取り消すには、**crypto ca server unrevoke** コマンドを入力します。証明書は、このコマンドによって証明書が証明書データベースで有効とマークされ、CRL から削除されると、再び有効になります。失効を取り消す証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書の失効が取り消された後に、CRL が自動的に再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書の失効を取り消す例を示します。

```
hostname(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked.A new CRL has been
issued.

hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db add

CA サーバのユーザ データベースに新しいユーザを挿入するには、特権 EXEC モードで **crypto ca server user-db add** コマンドを使用します。

crypto ca server user-db add *user* [**dn** *dn*] **[email** *e-mail-address*]

構文の説明

dn *dn*	追加するユーザに対して発行される証明書のサブジェクト名認定者名を指定します。DN ストリングにカンマが含まれる場合、値のストリングを二重引用符で囲みます（たとえば、O="Company, Inc."）。
email *e-mail-address*	新しいユーザの電子メール アドレスを指定します。
user	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

user 引数には単純なユーザ名（jandoe など）または電子メール アドレス（jandoe@example.com など）を指定できます。*username* は、エンド ユーザが登録ページで指定したユーザ名と一致する必要があります。

username は、特権のないユーザとしてデータベースに追加されます。登録特権を付与するには、**crypto ca server allow** コマンドを使用する必要があります。

username をワンタイム パスワードとともに使用して、登録インターフェイス ページでユーザを登録します。

（注） ワンタイム パスワード（OTP）を電子メールで通知するには、*username* フィールドまたは *email-address* フィールドに電子メール アドレスを指定する必要があります。メール送信時に電子メール アドレスが指定されていない場合、エラーが生成されます。

user 引数の **email** は、ユーザに登録と更新を忘れないように通知するための電子メール アドレスとしてのみ使用され、発行される証明書には表示されません。

電子メール アドレスを指定すると、質問がある場合にユーザに連絡することができ、また、その電子メール アドレス宛てに、登録に必要なワンタイム パスワードが通知されます。

ユーザにオプションの *dn* が指定されていない場合、サブジェクト名 dn は、*username* と subject-name-default DN 設定を使用して cn=*username*,subject-name-default として形成されます。

例

次に、ユーザ名 jandoe@example.com のユーザを完全なサブジェクト名 DN とともにユーザ データベースに追加する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db add dn "cn=Jan Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
hostname(config-ca-server)#
```

次に、jondoe というユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow jondoe
hostname(config-ca-server)
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、CA への登録を許可します。
crypto ca server user-db remove	CA サーバ データベースからユーザを削除します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。

crypto ca server user-db allow

ユーザまたはユーザのグループにローカル CA サーバ データベースへの登録を許可するには、特権 EXEC モードで **crypto ca server user-db allow** コマンドを使用します。このコマンドには、ワンタイム パスワードを生成および表示したり、ワンタイム パスワードをユーザに電子メールで送信したりするオプションも含まれています。

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]

構文の説明

all-certholders	証明書が現在有効かどうかに関係なく、証明書が発行されているデータベース内のすべてのユーザに登録特権を付与することを指定します。これは、更新特権の付与と同じです。
all-unenrolled	証明書が発行されていないデータベース内のすべてのユーザに登録特権を付与することを指定します。
email-otp	（任意）指定したユーザのワンタイム パスワードを、それらのユーザの設定済み電子メール アドレスに電子メールで送信します。
replace-otp	（任意）指定したユーザのうち、有効なワンタイム パスワードを当初は持っていたすべてのユーザに対してワンタイム パスワードを再生成することを指定します。
display-otp	（任意）指定したすべてのユーザのワンタイム パスワードをコンソールに表示します。
username	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

replace-otp キーワードを指定すると、指定したすべてのユーザに対して OTP が生成されます。指定したユーザに対して以前に生成された有効な OTP は、これらの新しい OTP で置き換えられます。

OTP は、セキュリティ デバイスに保存されませんが、ユーザに通知したり、登録時にユーザを認証したりする必要がある場合に生成および再生成されます。

例

次に、データベース内のすべての未登録ユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow all-unenrolled
hostname(config-ca-server)#
```

次に、user1 というユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow user1
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
enrollment-retrieval	登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db email-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットに OTP を電子メールで送信するには、特権 EXEC モードで **crypto ca server user-db email-otp** コマンドを使用します。

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

構文の説明

all-certholders	証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
username	1 人のユーザ用の OTP をそのユーザに電子メールで送信することを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、データベース内のすべての未登録ユーザに OTP を電子メールで送信する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
hostname(config-ca-server)#
```

次に、user1 というユーザに OTP を電子メールで送信する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db email-otp user1
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db show-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットのワンタイム パスワードを表示します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db remove

ローカル CA サーバのユーザ データベースからユーザを削除するには、特権 EXEC モードで **crypto ca server user-db remove** コマンドを使用します。

crypto ca server user-db remove *username*

構文の説明

username	削除するユーザの名前を、ユーザ名または電子メール アドレスの形式で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、CA ユーザ データベースからユーザ名を削除して、ユーザが登録できないようにします。また、このコマンドには、前に発行された有効な証明書を失効させるオプションもあります。

例

次に、ユーザ名 user1 のユーザを CA サーバのユーザ データベースから削除する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。

コマンド	説明
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報を、**database path** コマンドで指定したファイルに書き込みます。

crypto ca server user-db show-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットの OTP を表示するには、特権 EXEC モードで **crypto ca server user-db show-otp** コマンドを使用します。

crypto ca server user-db show-otp {*username* | **all-certholders** | **all-unenrolled**}

構文の説明

all-certholders	証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザの OTP を表示します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザの OTP を表示します。
username	1 人のユーザの OTP を表示することを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、有効または無効な証明書を持つデータベース内のすべてのユーザの OTP を表示する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db show-otp all-certholders
hostname(config-ca-server)#
```

次に、user1 というユーザの OTP を表示する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db show-otp user1
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db email-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットにワンタイム パスワードを電子メールで送信します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db write

すべてのローカル CA データベース ファイルを保存するディレクトリの場所を設定するには、特権 EXEC モードで **crypto ca server user-db write** コマンドを使用します。

crypto ca server user-db write

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

crypto ca server user-db write コマンドを使用して、新しいユーザベースのコンフィギュレーション データを、データベース パス コンフィギュレーションで指定した場所に保存します。この情報は、**crypto ca server user-db add** コマンドおよび **crypto ca server user-db allow** コマンドで新しいユーザが追加または許可されると生成されます。

例

次に、ローカル CA データベースに設定されているユーザ情報を保存場所に書き込む例を示します。

```
hostname(config-ca-server)# crypto ca server user-db write
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。

コマンド	説明
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca trustpoint

指定したトラストポイントのトラストポイント コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定したトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

構文の説明

noconfirm	すべての対話形式プロンプトを非表示にします。
trustpoint- name	管理するトラストポイントの名前を指定します。名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	Online Certificate Status Protocol をサポートするためにサブコマンドが追加されました。これらのサブコマンドには、**match certificate map**、**ocsp disable-nonce**、**ocsp url**、**revocation-check** が含まれます。
8.0(2)	証明書の検証をサポートするサブコマンドが追加されました。これらのサブコマンドには、**id-usage** と **validation-policy** が含まれます。**accept-subordinates**、**id-cert-issuer**、および **support-user-cert-validation** は廃止されました。
8.0(4)	信頼できるエンタープライズ間（Phone-Proxy と TLS-Proxy 間など）での自己署名証明書の登録をサポートするために、**enrollment self** サブコマンドが追加されました。

使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、クリプト CA トラストポイント コンフィギュレーション モードが開始されます。

このコマンドは、トラストポイント情報を管理します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラ

メータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

このコマンド リファレンス ガイドにアルファベット順で記載されている次のコマンドを使用して、トラストポイントの特性を指定できます。

- **accept-subordinates**：トラストポイントに関連付けられた CA に従属する CA 証明書がデバイスにインストールされていない場合、フェーズ 1 の IKE 交換中にその CA 証明書が提供されたときに、それを受け入れるかどうかを指定します。
- **client-types**：このトラストポイントを使用して、ユーザ接続に関連付けられた証明書を検証できるクライアント接続タイプを指定します。
- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。
- **crl configure**：CRL コンフィギュレーション モードを開始します（**crl** を参照）。
- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **enrollment retry period**：SCEP 登録の再試行期間を分単位で指定します。
- **enrollment retry count**：SCEP 登録に許可する最大試行回数を指定します。
- **enrollment self**：自己署名証明書を生成する登録を指定します。
- **enrollment terminal**：このトラストポイントへのカット アンド ペースト登録を指定します。
- **enrollment url** *url*：このトラストポイントに登録する SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **exit**：コンフィギュレーション モードを終了します。
- **fqdn** *fqdn*：登録中に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **id-cert-issuer**：廃止されました。このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **id-usage**：トラストポイントの登録済み ID の使用方法を指定します。
- **ignore-ipsec-keyusage**：廃止されました。IPsec クライアント証明書のキー使用チェックを行わないようにします。
- **ignore-ssl-keyusage**：廃止されました。SSL クライアント証明書のキー使用チェックを行わないようにします。
- **ip-addr** *ip-address*：登録中に、セキュリティ アプライアンスの IP アドレスを証明書に含めるかどうかを CA に確認します。
- **keypair** *name*：公開キーが証明対象となるキー ペアを指定します。
- **match certificate** *map-name* **override ocsp**：証明書マップを OCSP 上書きルールと照合します。
- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。ナンス拡張子は、失効要求と応答を結び付けて暗号化して、リプレイ アタックを回避するためのものです。
- **ocsp url**：この URL の OCSP サーバで、トラストポイントに関連するすべての証明書の失効ステータスをチェックすることを指定します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。
- **proxy-ldc-issuer**：TLS プロキシ ローカル ダイナミック証明書の発行者を指定します。

- **revocation check**：失効をチェックする方法（CRL、OCSP、none）を指定します。
- **serial-number**：登録中に、セキュリティ アプライアンスのシリアル番号を証明書に含めるかどうかを CA に確認します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。
- **support-user-cert-validation**：廃止されました。イネーブルの場合、リモート証明書を発行した CA に対してトラストポイントが認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定をこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL サブモードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。
- **validation-policy**：廃止されました。ユーザ接続に関連付けられている証明書を検証するためのトラストポイントの条件を指定します。

例

次に、central という名前のトラストポイントを管理するために CA トラストポイント モードを開始する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca certificate map	クリプト CA 証明書マップ モードを開始します。証明書ベースの ACL を定義します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。

crypto dynamic-map match address

アクセス リストのアドレスをダイナミック クリプト マップ エントリに一致させるには、グローバル コンフィギュレーション モードで **crypto dynamic-map match address** コマンドを使用します。アドレス一致をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

構文の説明

acl-name	ダイナミック クリプト マップ エントリに一致させるアクセス リストを指定します。
dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの詳細については、**crypto map match address** コマンドを参照してください。

例

次に、**crypto dynamic-map** コマンドを使用して、aclist1 という名前のアクセス リストのアドレスに一致させる例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto dynamic-map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの NAT-T をディセーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set peer

このコマンドの詳細については、**crypto map set peer** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。
ip_address	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアを IP アドレスで指定します。
hostname	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアをホスト名で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、mymap という名前のダイナミック マップのピアを IP アドレス 10.0.0.1 に設定する例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set pfs

ダイナミック クリプト マップ セットを指定するには、グローバル コンフィギュレーション モードで **crypto map dynamic-map set pfs** コマンドを使用します。指定したダイナミック クリプト マップ セットを削除するには、このコマンドの **no** 形式を使用します。

このコマンドの詳細については、**crypto map set pfs** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
set pfs	ダイナミック クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に Perfect Forward Secrecy（PFS; 完全転送秘密）を要求するように IPSec を設定するか、新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

crypto dynamic-map コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明します ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次に、ダイナミック クリプト マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用するよう指定する例を示します。指定されているグループはグループ 2 です。

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set reverse route

このコマンドの詳細については、crypto map set reverse-route コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

構文の説明

dynamic-map-name	クリプト マップ セットの名前を指定します。
dynamic-seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト値はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの RRI をイネーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set transform-set

ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set transform-set** コマンドを使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

ダイナミック クリプト マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式で、削除するトランスフォーム セットの名前を指定します。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

トランスフォーム セットをすべて指定するかまたは何も指定せずに、このコマンドの **no** 形式を使用すると、ダイナミック クリプト マップ エントリが削除されます。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。

使用上のガイドライン

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、欠落しているパラメータが、IPsec ネゴシエーションの結果として、ピアの要件に合うように後でダイナミックに学習されるポリシー テンプレートの役割を果たします。セ

キュリティ アプライアンスは、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。セキュリティ アプライアンスは、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています 一般に、LAN-to-LAN トンネルには、事前に決定済みのプライベート ネットワークのセットがあり、スタティック マップを設定し、IPSec SA を確立するために使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントは、スタティック IP アドレスを持たないため、IPSec ネゴシエーションを開始するためにダイナミック クリプト マップを必要とします。たとえば、ヘッドエンドが IKE のネゴシエーション中に Cisco VPN Client に IP アドレスを割り当て、クライアントはこのアドレスを IPSec SA のネゴシエーションで使用します。

ダイナミック クリプト マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ダイナミック クリプト マップは、ピアが常に事前に決定されるとは限らないネットワークで使用することを推奨します。ダイナミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

ヒント　ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネットのブロードキャスト トラフィック、および IPSec で保護されない他のすべてのトラフィックについて **deny** エントリを挿入するようにしてください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。セキュリティ アプライアンスは、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップを設定した場合は、発信トラフィックがアクセス リストの permit エントリに一致する場合でも、対応する SA が存在しないと、セキュリティ アプライアンスはそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック クリプト マップのセットには、クリプト マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、セキュリティ アプライアンスが他のクリプト マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック クリプト マップを含めます。dynamic-seq-num によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、クリプト アクセス リストに対して IPSec ピアのデータ フローを指定するために許可 ACL を挿入します。このように設定しないと、セキュリティ アプライアンスは、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意　ダイナミック クリプト マップ セットを使用して設定されたセキュリティ アプライアンス インターフェイスにトンネリングされるトラフィックに対してスタティック（デフォルト）ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

1 つのクリプト マップ セット内で、スタティック マップ エントリとダイナミック マップ エントリを組み合わせることができます。

例

次に、10 個の同じトランスフォーム セットから成る「dynamic0」というダイナミック クリプト マップ エントリを作成する例を示します。「crypto ipsec transform-set（トランスフォーム セットの作成または削除)」の項には、10 個のトランスフォーム セット サンプル コマンドが示されています。

```
hostname(config)# crypto dynamic-map dynamic0 1 set transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec transform-set	トランスフォーム セットを設定します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto ipsec df-bit

IPSec パケットの DF-bit ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

構文の説明

clear-df	（任意）外部 IP ヘッダーで DF ビットがクリアされること、およびセキュリティ アプライアンスはパケットをフラグメント化して IPSec カプセル化を追加する場合があることを指定します。
copy-df	（任意）セキュリティ アプライアンスが外部 DF ビット設定を元のパケット内で探すことを指定します。
set-df	（任意）外部 IP ヘッダーに DF ビットを設定することを指定します。ただし、元のパケットで DF ビットがクリアされている場合、セキュリティ アプライアンスはパケットをフラグメント化することがあります。
interface	インターフェイス名を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。設定を指定せずにこのコマンドをイネーブルにすると、セキュリティ アプライアンスはデフォルトとして **copy-df** 設定を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

DF ビットを IPSec トンネル機能とともに使用すると、セキュリティ アプライアンスが、カプセル化されたヘッダーで Don't Fragment（DF）ビットをクリア、設定、またはコピーできるかどうかを指定できます。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダーに DF ビットを指定するようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。

トンネル モードの IPSec トラフィックをカプセル化する場合は、DF ビットに **clear-df** 設定を使用します。この設定を使用すると、デバイスは、使用可能な MTU サイズよりも大きなパケットを送信できます。また、この設定は、使用可能な MTU サイズが不明な場合にも適しています。

例

次に、グローバル コンフィギュレーション モードで、IPSec DF ポリシーを **clear-df** に設定する例を示します。

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。
show crypto ipsec fragmentation	指定したインターフェイスのフラグメンテーション ポリシーを表示します。

crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec fragmentation** コマンドを使用します。

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

構文の説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPSec パケットをセキュリティ アプライアンスがフラグメント化するように指定します（事前フラグメント化をディセーブルにします）。
before-encryption	暗号化の前に MTU の最大サイズに近い IPSec パケットをセキュリティ アプライアンスがフラグメント化するように指定します（事前フラグメント化をイネーブルにします）。
interface	インターフェイス名を指定します。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

パケットは、暗号化するセキュリティ アプライアンスの発信リンクの MTU サイズに近い場合、IPSec ヘッダーを付けてカプセル化されると、発信リンクの MTU を超える可能性があります。超えた場合は、暗号化の後にパケットがフラグメント化され、復号化デバイスがプロセス パスで再構築することになります。IPSec VPN の事前フラグメント化では、デバイスはプロセス パスではなく高性能な CEF パスで動作するため、復号化時のデバイスのパフォーマンスが向上します。

IPSec VPN の事前フラグメント化により、暗号化デバイスは、IPSec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。デバイスでパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、デバイスは暗号化する前にそのパケットをフラグメント化します。これにより、復号化前にプロセス レベルでパケットを再構築する必要がなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

例

次に、グローバル コンフィギュレーション モードで、IPSec パケットの事前フラグメント化をデバイス上でグローバルにイネーブルにする例を示します。

```
hostname(config)# crypto ipsec fragmentation before-encryption inside
```

```
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、IPSec パケットの事前フラグメント化をインターフェイス上でディセーブルにする例を示します。

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

crypto ipsec security-association lifetime

グローバル ライフタイム値を設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association lifetime** コマンドを使用します。crypto ipsec エントリのライフタイム値をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

構文の説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。デフォルトは 4,608,000 KB です。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。デフォルトは 28,800 秒（8 時間）です。
token	ユーザ認証にトークンベースのサーバを使用することを指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

crypto ipsec security-association lifetime コマンドは、IPSec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル ライフタイム値を変更します。

IPSec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

個々のクリプト マップ エントリでライフタイム値が設定されていない場合、セキュリティ アプライアンスは、ネゴシエート中に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求の中でグローバル ライフタイム値を指定します。セキュリティ アプライアンスは、この値を新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、「期間」ライフタイムと、「トラフィック量」ライフタイムの 2 種類があります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。

セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定をオンザフライで変更できます。変更された場合、セキュリティ アプライアンスでは、変更によって影響を受ける接続のみが切断されます。クリプト マップに関連付けられている既存のアクセス リストをユーザが変更した場合（たとえばアクセス リスト内のエントリを削除した場合）、関連する接続のみが切断されます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

グローバルな指定時刻ライフタイムを変更するには、**crypto ipsec security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にセキュリティ アソシエーションがタイムアウトします。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用すると、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された後に、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、同一キーで暗号化されている解析対象データが少なくなるため、攻撃者はキー回復攻撃を開始することが難しくなります。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（および対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、いずれかを最初に超えた時点で有効期限が切れます。

例

次に、セキュリティ アソシエーションのグローバル指定時刻ライフタイムを指定する例を示します。

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）をクリアします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

crypto ipsec security-association replay

IPSec アンチリプレイ ウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association replay** コマンドを使用します。ウィンドウ サイズをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association replay {**window-size** *n* | **disable**}

no crypto ipsec security-association replay {**window-size** *n* | **disable**}

構文の説明

n	ウィンドウ サイズを設定します。指定できる値は、64、128、256、512、または 1024 です。デフォルト値は 64 です。
disable	アンチリプレイ チェックをディセーブルにします。

デフォルト

デフォルトのウィンドウ サイズは 64 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチ リプレイ保護が提供されます（セキュリティ アソシエーションのアンチ リプレイは、受信者が過去のパケットや複製されたパケットを拒否することによりリプレイ アタックを防ぐセキュリティ サービスです）。復号化側では、検知したことのあるシーケンス番号は破棄されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N のパケットはすべて廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、QoS はプライオリティが高いパケットを優先しますが、これにより、プライオリティが低いパケットが、デクリプタによって受信された最後の 64 パケットの 1 つであっても、廃棄される場合があります。このイベントにより、誤ったアラームである警告 syslog メッセージが生成される可能性があります。**crypto ipsec security-association replay** コマンドを使用すると、ウィンドウ サイズを拡張して、デクリプタが 64 を超えるパケットを追跡できます。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

例

次に、セキュリティ アソシエーションのアンチリプレイ ウィンドウ サイズを指定する例を示します。

```
hostname(config)# crypto ipsec security-association replay window-size 1024
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）をクリアします。
shape	トラフィック シェーピングをイネーブルにします。
priority	プライオリティ キューイングをイネーブルにします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

crypto ipsec transform-set（トランスフォーム セットの作成または削除）

トランスフォーム セットを作成または削除するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。**crypto ipsec transform-set** コマンドを使用すると、トランスフォーム セットで使用される IPSec 暗号化およびハッシュ アルゴリズムを指定できます。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

no crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

構文の説明

authentication	（任意）IPSec のデータ フローの整合性を保証する認証方法を次の中から 1 つ指定します。 **esp-md5-hmac**：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。 **esp-sha-hmac**：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。 **esp-none**：HMAC 認証を使用しない場合。
encryption	IPSec のデータ フローを保護する暗号化方法を次の中から 1 つ指定します。 **esp-aes**：128 ビット キーで AES を使用する場合。 **esp-aes-192**：192 ビット キーで AES を使用する場合。 **esp-aes-256**：256 ビット キーで AES を使用する場合。 **esp-des**：56 ビットの DES-CBC を使用する場合。 **esp-3des**：トリプル DES アルゴリズムを使用する場合。 **esp-null**：暗号化を使用しない場合。
transform-set-name	作成または変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

デフォルトの認証設定は、esp-none（認証しない）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	この項は書き換えられました。

使用上のガイドライン

トランスフォーム セットを設定したら、そのセットをクリプト マップに割り当てます。1 つのクリプト マップに対して最大 6 つのトランスフォーム セットを割り当てることができます。ピアが IPSec セッションを確立しようとすると、セキュリティ アプライアンスは、一致が検出されるまで、各クリプト マップのアクセス リストに照らしてピアを評価します。次に、セキュリティ アプライアンスは、一致が検出されるまで、ピアがネゴシエートするすべてのプロトコル、アルゴリズム、およびその他の設定を、クリプト マップに割り当てられているトランスフォーム セット内の設定に照らして評価します。セキュリティ アプライアンスでは、ピアの IPSec ネゴシエーションとトランスフォーム セット内の設定とが一致すると、IPSec セキュリティ アソシエーションの一部としてその設定を保護されたトラフィックに適用します。セキュリティ アプライアンスは、ピアがアクセス リストに一致しない場合や、クリプト マップに割り当てられているトランスフォーム セット内にピアのセキュリティ設定と完全に一致するセキュリティ設定が見つからない場合、IPSec セッションを終了します。

暗号化と認証のどちらを先に指定してもかまいません。認証を指定せずに暗号化を指定することもできます。作成するトランスフォーム セットに認証を指定する場合は、暗号化も指定する必要があります。変更するトランスフォーム セットに認証だけを指定した場合、トランスフォーム セットでは、現在の暗号化設定が維持されます。

AES 暗号化を指定する場合は、グローバル コンフィギュレーション モードでも **isakmp policy priority group 5** コマンドを使用して、AES で提供される大きなキー サイズに対応できるように Diffie-Hellman グループ 5 を割り当てることを推奨します。

ヒント

クリプト マップまたはダイナミック クリプト マップにトランスフォーム セットを適用し、そのマップに割り当てられているトランスフォーム セットを表示する場合は、トランスフォーム セットにコンフィギュレーションの内容を表す名前を付けておくと便利です。たとえば、次に示す最初の例の「3des-md5」は、トランスフォーム セットで使用する暗号化と認証を示しています。この名前の後に続く値は、トランスフォーム セットに割り当てる実際の暗号化と認証の設定です。

例

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
hostname(config)# crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 56des-md5 esp-des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 56des-sha esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 128aes-md5 esp-aes esp-md5-hmac
hostname(config)# crypto ipsec transform-set 128aes-sha esp-aes esp-sha-hmac
hostname(config)# crypto ipsec transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 192aes-sha esp-aes-192 esp-sha-hmac
hostname(config)# crypto ipsec transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 256aes-sha esp-aes-256 esp-sha-hmac
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。

コマンド	説明
crypto map set transform-set	クリプトマップエントリで使用するトランスフォーム セットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。

crypto isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp am-disable

no crypto isakmp am-disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp am-disable** コマンドが追加されました。
7.2.(1)	**isakmp am-disable** コマンドが、**crypto isakmp am-disable** コマンドに置き換えられました。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
hostname(config)# crypto isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp disconnect-notify

ピアに対する切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp disconnect-notify** コマンドが追加されました。
7.2.(1)	**isakmp disconnect-notify** コマンドが、**crypto isakmp disconnect-notify** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# crypto isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp enable** コマンドを使用します。インターフェイスで ISAKMP をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp enable *interface-name*

no crypto isakmp enable *interface-name*

構文の説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	**isakmp enable** コマンドは既存のものです。
7.2(1)	**isakmp enable** コマンドが、**crypto isakmp enable** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no crypto isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp identity

フェーズ 2 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **crypto isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISAKMP ネゴシエーションを、接続のタイプ（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）によって判別します。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

デフォルト

デフォルトの ISAKMP ID は、**crypto isakmp identity auto** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	**isakmp identity** コマンドは既存のものです。
7.2(1)	**isakmp identity** コマンドが、**crypto isakmp identity** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

```
hostname(config)# crypto isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。

コマンド	説明
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

no crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	（任意）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp ipsec-over-tcp** コマンドが追加されました。
7.2.(1)	**isakmp ipsec-over-tcp** コマンドが、**crypto isakmp ipsec-over-tcp** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、IPSec over TCP をポート 45 でイネーブルにします。

```
hostname(config)# crypto isakmp ipsec-over-tcp port 45
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp nat-traversal

NAT トラバーサルをグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることを確認します（イネーブルにするには **crypto isakmp enable** コマンドを使用します）。NAT トラバーサルをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトでは、NAT トラバーサルはイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp nat-traversal** コマンドは既存のものです。
7.2.(1)	**isakmp nat-traversal** コマンドが、**crypto isakmp nat-traversal** コマンドに置き換えられました。
8.0(2)	NAT トラバーサルが、デフォルトでイネーブルになりました。

使用上のガイドライン

NAT（PAT を含む）は、IPSec も使用されている多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを正常に通過することを妨げる非互換性が数多くあります。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおりに NAT トラバーサルをサポートしています。また、ダイナミック クリプト マップとスタティック クリプト マップの両方で NAT トラバーサルをサポートしています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、NAT トラバーサルのキープアライブ間隔を 30 秒に設定する例を示します。

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

構文の説明

crack	認証方式として、IKE CRACK を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy authentication** コマンドは既存のものです。
7.2.(1)	**isakmp policy authentication** コマンドが、**crypto isakmp policy authentication** コマンドに置き換えられました。

使用上のガイドライン

RSA シグニチャを指定する場合は、CA サーバから証明書を取得するようにセキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy authentication** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーで RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy encryption

IKE ポリシーで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no crypto isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy encryption** コマンドは既存のものです。
7.2.(1)	**isakmp policy encryption** コマンドが、**crypto isakmp policy encryption** コマンドに置き換えられました。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy encryption** コマンドを使用する例を示します。この例では、プライオリティ番号 25 の IKE ポリシーに使用するアルゴリズムとして 128 ビット キーの AES 暗号化を設定します。

```
hostname(config)# crypto isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 encryption 3des
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **group** {**1 | 2 | 5**}

no crypto isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトのグループ ポリシーはグループ 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy group** コマンドが追加されました。
7.2(1)	**isakmp policy group** コマンドが、**crypto isakmp policy group** コマンドに置き換えられました。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注）　Cisco VPN Client のバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります （DH グループ 1 に設定すると、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）グループ 1 やグループ 2 ではなく、グループ 5 を使用する必要があります。グループ 5 を設定するには、**crypto isakmp policy priority group 5** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

```
hostname(config)# crypto isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **hash** {**md5 | sha**}

no crypto isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーのハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。
priority	プライオリティをポリシーに一意に指定および割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーのハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy hash** コマンドは既存のものです。
7.2.(1)	**isakmp policy hash** コマンドが、**crypto isakmp policy hash** コマンドに置き換えられました。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy hash** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# crypto isakmp policy 40 hash  md5
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy lifetime

IKE セキュリティ アソシエーションが期限切れになるまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy lifetime** コマンドを使用します。ピアがライフタイムを提示していない場合は、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

構文の説明

priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy lifetime** コマンドは既存のものです。
7.2.(1)	**isakmp policy lifetime** コマンドが、**crypto isakmp policy lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

（注）　IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。

例

次に、グローバル コンフィギュレーション モードで、プライオリティ番号 40 の IKE ポリシーに IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 lifetime 0
```

関連コマンド

clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp reload-wait

すべてのアクティブなセッションが自発的に終了しないとセキュリティ アプライアンスをリブートできないようにするは、グローバル コンフィギュレーション モードで **crypto isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずにセキュリティ アプライアンスをリブートするには、このコマンドの **no** 形式を使用します。

crypto isakmp reload-wait

no crypto isakmp reload-wait

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp reload-wait** コマンドが追加されました。
7.2.(1)	**isakmp reload-wait** コマンドが、**crypto isakmp reload-wait** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからセキュリティ アプライアンスをリブートするように設定します。

```
hostname(config)# crypto isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto key generate rsa

アイデンティティ証明書用の RSA キー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

構文の説明

general-keys	1 つの汎用キー ペアを生成します。これはデフォルトのキー ペア タイプです。
label *key-pair-label*	キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。同じラベルを使用して別のキー ペアを作成しようとすると、セキュリティ アプライアンスは警告メッセージを表示します。キーの生成時にラベルを指定しない場合、そのキー ペアにはスタティックに <Default-RSA-Key> という名前が付けられます。
modulus *size*	キー ペアのモジュラス サイズ（512、768、1024、および 2048）を指定します。デフォルトのモジュラス サイズは 1024 です。
noconfirm	すべての対話型プロンプトを非表示にします。
usage-keys	シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 つの証明書が必要なことを意味します。

デフォルト

デフォルトのキー ペア タイプは、**general key** です。デフォルトのモジュラス サイズは 1024 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートするために RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。生成されたキー ペアは、コマンド構文の一部として指定できるラベルで識別されます。キー ペアを参照しないトラストポイントは、デフォルトの <Default-RSA-Key> を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、証明書やキーがトラストポイントに設定されていない限り、このことは SSL に影響を与えません。

注意　1024 ビットを超える RSA キー ペアを持つ ID 証明書を使用している複数の SSL 接続によって、セキュリティ アプライアンスでの CPU 使用率が高くなり、クライアントレス ログインが拒否される可能性があります。

例

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの RSA キー ペアを生成する例を示します。

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルが重複する RSA キー ペアを誤って生成しようとする例を示します。

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、デフォルト ラベルの RSA キー ペアを生成する例を示します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key zeroize	RSA キー ペアを削除します。
show crypto key mypubkey	RSA キー ペアを表示します。

crypto key zeroize

指定したタイプ（rsa または dsa）のキー ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize** コマンドを使用します。

crypto key zeroize {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

構文の説明

default	ラベルがない RSA キー ペアを削除します。このキーワードは、RSA キー ペアに限り有効です。
dsa	キー タイプとして DSA を指定します。
label *key-pair-label*	指定したタイプ（rsa または dsa）のキー ペアを削除します。ラベルを指定しない場合、セキュリティ アプライアンスは、指定したタイプのキー ペアをすべて削除します。
noconfirm	すべての対話型プロンプトを非表示にします。
rsa	キー タイプとして RSA を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、グローバル コンフィギュレーション モードで、すべての RSA キー ペアを削除する例を示します。

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key generate dsa	アイデンティティ証明書用の DSA キー ペアを生成します。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。

crypto map interface

以前に定義したクリプト マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで **crypto map interface** コマンドを使用します。このクリプト マップ セットをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

構文の説明

interface-name	セキュリティ アプライアンスが VPN ピアとのトンネルの確立に使用するインターフェイスを指定します。ISAKMP がイネーブルになっており、CA を使用して証明書を取得する場合は、CA 証明書で指定されているアドレスを持つインターフェイスにする必要があります。
map-name	クリプト マップ セットの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドを使用して、クリプト マップ セットを任意のアクティブなセキュリティ アプライアンスのインターフェイスに割り当てます。セキュリティ アプライアンスでは、あらゆるアクティブ インターフェイスを IPSec の終端にすることができます。インターフェイスで IPSec サービスを提供するには、そのインターフェイスにまずクリプト マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができるクリプト マップ セットは 1 つだけです。同じ *map-name* で *seq-num* が異なるクリプト マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、そのインターフェイスにすべて適用されます。セキュリティ アプライアンスは、*seq-num* が最も小さいクリプト マップ エントリを最初に評価します。

（注）　セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、クリプト マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続のみが停止させられます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

すべてのスタティック クリプト マップでは、アクセス リスト、トランスフォーム セット、および IPsec ピアという 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、そのクリプト マップは不完全であるため、セキュリティ アプライアンスは次のエントリに進みます。ただし、クリプト マップがアクセス リストでは一致するが、他の 2 つの要件のいずれかまたは両方で一致しない場合、セキュリティ アプライアンスはトラフィックをドロップします。

すべてのクリプト マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ セットを外部インターフェイスに割り当てる例を示します。トラフィックは、この外部インターフェイスを通過するとき、セキュリティ アプライアンスによって mymap セット内のすべてのクリプト マップ エントリに照らして評価されます。発信トラフィックが、いずれかの mymap クリプト マップ エントリのアクセス リストと一致する場合、セキュリティ アプライアンスはそのクリプト マップ エントリのコンフィギュレーションを使用して、セキュリティ アソシエーションを形成します。

```
hostname(config)# crypto map mymap interface outside
```

次に、必要最小限のクリプト マップ エントリ コンフィギュレーションの例を示します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map ipsec-isakmp dynamic

所定のクリプト マップ エントリで既存のダイナミック クリプト マップを参照させるようにするには、グローバル コンフィギュレーション モードで **crypto map ipsec-isakmp dynamic** コマンドを使用します。相互参照を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック クリプト マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック クリプト マップ セットを作成した後に、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック クリプト マップ セットをスタティック クリプト マップに追加します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

構文の説明

dynamic-map-name	既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。
ipsec-isakmp	IKE がクリプト マップ エントリの IPSec セキュリティ アソシエーションを確立することを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドは、**ipsec-manual** キーワードを削除するように変更されました。

使用上のガイドライン

クリプト マップ エントリを定義してから、**crypto map interface** コマンドを使用して、ダイナミック クリプト マップ セットをインターフェイスに割り当てることができます。

ダイナミック クリプト マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番めの機能はそのトラフィックのために（IKE を通じて）実行されるネゴシエーションが対象となります。

IPSec ダイナミック クリプト マップでは、次のことを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPSec ピア

- 保護対象のトラフィックとともに使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

クリプト マップ セットとは、それぞれ異なるシーケンス番号（seq-num）を持つが、マップ名が同じであるクリプト マップ エントリの集合です。したがって、所定のインターフェイスで、あるトラフィックには指定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPSec セキュリティを適用して同じまたは別のピアに転送できます。これを行うには、マップ名は同じであるが、シーケンス番号がそれぞれ異なる 2 つのクリプト マップ エントリを作成します。

seq-num 引数として割り当てる番号は、任意に決定しないでください。この番号によって、クリプト マップ セット内の複数のクリプト マップ エントリにランクが付けられます。小さいシーケンス番号のクリプト マップ エントリは、大きいシーケンス番号のマップ エントリよりも先に評価されます。つまり、番号の小さいマップ エントリの方がプライオリティが高くなります。

（注）　クリプト マップをダイナミック クリプト マップにリンクする場合は、ダイナミック クリプト マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック クリプト マップにクリプト マップがリンクされます。クリプト マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。ただし、セキュリティ アプライアンスは起動中に変更を保存します。ダイナミック クリプト マップをクリプト マップに変換して戻す場合、この変更は有効となり、**show running-config crypto map** コマンドの出力に表示されます。セキュリティ アプライアンスは、リブートされるまでこれらの設定を維持します。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、test という名前のダイナミック クリプト マップを参照するようにクリプト マップ mymap を設定します。

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map match address

アクセス リストをクリプト マップ エントリに割り当てるには、グローバル コンフィギュレーション モードで **crypto map match address** コマンドを使用します。クリプト マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

構文の説明

acl_name	暗号化アクセス リストの名前を指定します。この名前は、一致対象となる名前付き暗号化アクセス リストの名前引数と一致している必要があります。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、すべてのスタティック クリプト マップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップを定義する場合、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセス リストを定義するには、**access-list** コマンドを使用します。アクセス リストのヒット カウントは、トンネルが開始されたときにのみ増加します。トンネルがいったんアップ状態になると、ヒット カウントはパケット フローごとには増加しません。トンネルがドロップされてから再開されると、ヒット カウントは増加します。

セキュリティ アプライアンスは、アクセス リストを使用して、IPSec クリプトで保護するトラフィックと保護を必要としないトラフィックとを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが確実に保護されるようにします。

セキュリティ アプライアンスは、パケットが deny ステートメントと一致すると、クリプト マップ内の残りの ACE に対するパケットの評価を省略して、順番に次のクリプト マップ内の ACE に対するパケットの評価を再開します。*ACL のカスケード処理*には、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用、およびクリプト マップ セット内の次のクリプト マップに割り当てられた ACL に対するトラフィックの評価の再開が含まれています。各クリプト マップを異なる IPSec 設定に関連付

けることができるため、拒否 ACE を使用して、対応するクリプト マップの詳細な評価から特別なトラフィックを除外し、その特別なトラフィックを別のクリプト マップの permit ステートメントに一致させることで別のセキュリティを提供または要求できます。

（注） クリプト アクセス リストでは、インターフェイスを通過するトラフィックを許可するかどうかは判別されません。このような判別は、**access-group** コマンドを使用してインターフェイスに直接適用されるアクセス リストによって行われます。

トランスペアレント モードでは、宛先アドレスはセキュリティ アプライアンスの IP アドレス、管理アドレスである必要があります。トランスペアレント モードでは、セキュリティ アプライアンスへのトンネルだけが許可されます。

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set connection-type

クリプト マップ エントリのバックアップ Site-to-Site 機能の接続タイプを指定するには、グローバル コンフィギュレーション モードで **crypto map set connection-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

no crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

構文の説明

answer-only	ピアが、適切な接続先ピアを決定するための最初の独自の交換中に、まず着信 IKE 接続だけに応答することを指定します。
bidirectional	ピアが、クリプト マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これは、すべての Site-to-Site 接続のデフォルトの接続タイプです。
map-*name*	クリプト マップ セットの名前を指定します。
originate-only	ピアが、適切な接続先ピアを決定するために最初の独自の交換を開始することを指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set connection-type	クリプト マップ エントリのバックアップ Site-to-Site 機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 つのタイプの接続があります。

デフォルト

デフォルトの設定は bidirectional です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

crypto map set connection-type コマンドは、バックアップ Lan-to-Lan 機能の接続タイプを指定します。接続の一方の側で複数のバックアップ ピアを指定できます。

この機能は、次のプラットフォーム間でのみ使用できます。

- 2 つの Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと Cisco VPN 3000 コンセントレータ

- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと、Cisco PIX セキュリティ アプライアンス ソフトウェア v7.0 以上を実行しているセキュリティ アプライアンス

バックアップ Lan-to-Lan 接続を設定するには、接続の一方の側を **originate-only** キーワードを使用して originate-only として設定し、複数のバックアップ ピアがある側を **answer-only** キーワードを使用して answer-only として設定することを推奨します。originate-only 側では、**crypto map set peer** コマンドを使用してピアのプライオリティを指定します。originate-only セキュリティ アプライアンスは、リストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

このように設定した場合、originate-only ピアは、最初に独自のトンネルを確立してピアとネゴシエートしようとします。その後は、いずれかのピアが通常の Lan-to-Lan 接続を確立することができ、いずれかの側からのデータがトンネル接続を開始できます。

トランスペアレント ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられたクリプト マップに含まれるクリプト マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

表 9-1 に、サポートされているすべてのコンフィギュレーションを示します。他の組み合わせは、予測不可能なルーティング問題を引き起こす場合があります。

表 9-1　サポートされているバックアップ LAN-to-LAN 接続タイプ

リモート側	中央側
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、接続タイプを originate-only に設定する例を示します。

```
hostname(config)# crypto map mymap 10 set connection-type originate-only
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set inheritance

クリプト マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）を設定するには、グローバル コンフィギュレーション モードで **set inheritance** コマンドを使用します。クリプト マップ エントリの継承の設定を削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set inheritance {data| rule}**

no crypto map *map-name seq-num* **set inheritance {data | rule}**

構文の説明

data	ルールで指定されているアドレス範囲内のアドレス ペアごとに 1 つのトンネルを指定します。
map-name	クリプト マップ セットの名前を指定します。
rule	クリプト マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これがデフォルトです。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプを **data** または **rule** に指定します。継承では、各 Security Policy Database（SPD; セキュリティ ポリシー データベース）ルールに対して 1 つの Security Association（SA; セキュリティ アソシエーション）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。

デフォルト

デフォルト値は、**rule** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンスがトンネルに応答しているときではなく、トンネルを開始しているときにのみ機能します。データ設定を使用すると、多数の IPSec SA が作成される可能性があります。この場合、メモリが消費され、全体としてのトンネルが少なくなります。データ設定は、セキュリティへの依存が非常に高いアプリケーションに対してのみ使用してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、継承タイプを data に設定する例を示します。

```
hostname(config)# crypto map mymap 10 set inheritance data
```

```
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ エントリの NAT-T をディセーブルにします。

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
isakmp nat-traversal	すべての接続の NAT-T をイネーブルにします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set peer

クリプト マップ エントリの IPSec ピアを指定するには、グローバル コンフィギュレーション モードで **crypto map set peer** コマンドを使用します。クリプト マップ エントリから IPSec ピアを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

構文の説明

hostname	ピアを、セキュリティ アプライアンスの **name** コマンドで定義したホスト名で指定します。
ip_address	ピアを IP アドレスで指定します。
map-name	クリプト マップ セットの名前を指定します。
peer	クリプト マップ エントリの IPSec ピアをホスト名または IP アドレスで指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドは、最大 10 個のピア アドレスを許容するように変更されました。

使用上のガイドライン

このコマンドは、すべてのスタティック クリプト マップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップ エントリを定義する場合、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

複数のピアを設定することは、フォールバック リストを指定することと同じです。トンネルごとに、セキュリティ アプライアンスはリスト内の最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり、クリプト マップ接続タイプが originate-only の場合）にのみ複数のピアを設定できます。詳細については、**crypto map set connection-type** コマンドを参照してください。

例

次に、グローバル コンフィギュレーション モードで、IKE を使用してセキュリティ アソシエーションを確立するクリプト マップ コンフィギュレーションの例を示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 に対するセキュリティ アソシエーションを設定できます。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set pfs

クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に PFS を要求するように IPSec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec を設定するには、グローバル コンフィギュレーション モードで **crypto map set pfs** コマンドを使用します。IPSec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

構文の説明

group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、クリプト マップ エントリ用の新しいセキュリティ アソシエーションを要求するとき、ネゴシエート中に IPSec が PFS を要求します。**set pfs** ステートメントでグループが指定されていない場合、セキュリティ アプライアンスはデフォルト（グループ 2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションでグループ 2 またはグループ 5 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合、ネゴシエーションは失敗します。

ネゴシエーションが成功するには、両端に PFS が設定されている必要があります。設定されている場合、グループは完全に一致する必要があります。セキュリティ アプライアンスは、ピアからの PFS のいずれのオファーも受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループであるグループ 5 は、グループ 1 やグループ 2 よりも高いセキュリティを提供します。ただし、他のグループより処理時間が長くなります。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ「mymap 10」用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定する例を示します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
tunnel-group	トンネル グループとそのパラメータを設定します。

crypto map set phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKE モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set phase1 mode** コマンドを使用します。フェーズ 1 IKE ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、セキュリティ アプライアンスはグループ 2 を使用します。

crypto map *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

no crypto map *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

構文の説明

aggressive	フェーズ 1 IKE ネゴシエーションにアグレッシブ モードを指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
main	フェーズ 1 IKE ネゴシエーションにメイン モードを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

フェーズ 1 のデフォルト モードは **main** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設定する例を示します。

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set reverse-route

クリプト マップ エントリに基づいて任意の接続の RRI をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto map set reverse-route** コマンドを使用します。クリプト マップ エントリに基づいた任意の接続の逆ルート注入をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set reverse-route**

no crypto map *map-name seq-num s***et reverse-route**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知できます。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップの RRI をイネーブルにする例を示します。

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set security-association lifetime

特定のクリプト マップ エントリについて、IPSec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。クリプト マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

構文の説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。 デフォルトは 4,608,000 KB です。
map-name	クリプト マップ セットの名前を指定します。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

クリプト マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPSec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、セキュリティ アプライアンスは、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアか

らネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

ライフタイムには、「期間」ライフタイムと、「トラフィック量」ライフタイムの 2 種類があります。セッション キーとセキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。1 つのコマンドで両方を指定できます。

（注） セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、クリプト マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続のみが停止させられます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

指定時刻ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にキーおよびセキュリティ アソシエーションがタイムアウトします。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、クリプト マップ mymap のセキュリティ アソシエーション ライフタイムを秒単位および KB 単位で指定します。

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set transform-set

クリプト マップ エントリで使用するトランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto map set transform-set** コマンドを使用します。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

クリプト マップ エントリから特定のトランスフォーム セット名を削除するには、トランスフォーム セットの名前を指定してこのコマンドの **no** 形式を使用します。

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

トランスフォーム セットをすべて指定するか何も指定せずに、クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

no crypto map *map-name seq-num* **set transform-set**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。

使用上のガイドライン

このコマンドは、すべてのクリプト マップ エントリで必要です。

IPSec の開始側とは反対側にあるピアは、最初に一致したトランスフォーム セットをセキュリティ アソシエーションに使用します。ローカルのセキュリティ アプライアンスがネゴシエーションを開始した場合、セキュリティ アプライアンスは、**crypto map** コマンドで指定した順番どおりに、トランス

フォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルのセキュリティ アプライアンスは、クリプト マップ エントリ内の、ピアから送信された IPSec パラメータと一致する最初のトランスフォーム セットを使用します。

IPSec の開始側とは反対側にあるピアが、一致するトランスフォーム セットの値を見つけられない場合、IPSec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションがないため、開始側はトラフィックをドロップします。

トランスフォーム セットのリストを変更するには、新しいリストを再度指定して、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、セキュリティ アプライアンスは、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、セキュリティ アプライアンスは、「56des-sha」というトランスフォーム セットをリストの最後に挿入します。

```
hostname(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
hostname(config)# crypto map map1 1 transform-set 56des-sha
hostname(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
hostname(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

クリプト マップ エントリ内のトランスフォーム セットの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の map2 というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

「crypto ipsec transform-set（トランスフォーム セットの作成または削除）」の項には、10 個のトランスフォーム セット サンプル コマンドが示されています。次に、10 個の同じトランスフォーム セットから成る「map2」というクリプト マップ エントリを作成する例を示します。

```
hostname(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、セキュリティ アプライアンスが IKE を使用してセキュリティ アソシエーションを確立する場合に最小限必要となるクリプト マップ コンフィギュレーションの例を示します。

```
hostname(config)# crypto map map2 10 ipsec-isakmp
hostname(config)# crypto map map2 10 match address 101
hostname(config)# crypto map map2 set transform-set 3des-md5
hostname(config)# crypto map map2 set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。

コマンド	説明
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set trustpoint

クリプト マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定するトラストポイントを指定するには、グローバル コンフィギュレーション モードで **crypto map set trustpoint** コマンドを使用します。クリプト マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

構文の説明

chain	（任意）証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書からアイデンティティ証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル（チェーンなし）です。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
trustpoint-name	フェーズ 1 ネゴシエーション中に送信する証明書を指定します。デフォルトは none です。
token	ユーザ認証にトークンベースのサーバを使用することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このクリプト マップ コマンドは、接続の開始に対してのみ有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap に tpoint1 という名前のトラストポイントを指定し、証明書のチェーンを含める例を示します。

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
tunnel-group	トンネル グループを設定します。

csc

セキュリティ アプライアンスがネットワーク トラフィックを CSC SSM に送信できるようにするには、クラス コンフィギュレーション モードで **csc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

csc {**fail-open** | **fail-close**}

no csc

構文の説明

fail-close	CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックをブロックする必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。
fail-open	CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックを許可する必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

csc コマンドは、該当するクラス マップに一致したすべてのトラフィックを CSC SSM に送信するようにセキュリティ ポリシーを設定します。この設定の後、セキュリティ アプライアンスは、トラフィックが宛先に引き続き送信されるのを許可します。

CSC SSM がトラフィックをスキャンできない場合は、一致しているトラフィックをセキュリティ アプライアンスが処理する方法を指定できます。**fail-open** キーワードは、CSC SSM を使用できない場合でも、トラフィックが宛先に引き続き送信されるのをセキュリティ アプライアンスが許可するように指定します。**fail-close** キーワードは、CSC SSM が使用できない場合、一致しているトラフィックが宛先に引き続き送信されるのをセキュリティ アプライアンスが許可しないように指定します。

CSC SSM は、HTTP、SMTP、POP3、および FTP トラフィックをスキャンできます。接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のポートである場合にのみ、これらのプロトコルがサポートされます。つまり、CSC SSM は、次の接続のみをスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続。
- TCP ポート 80 に対してオープンされている HTTP 接続。
- TCP ポート 110 に対してオープンされている POP3 接続。
- TCP ポート 25 に対してオープンされている SMTP 接続。

csc コマンドを使用しているポリシーで、これらのポートを他のプロトコルに誤用する接続が選択された場合、セキュリティ アプライアンスはパケットを CSC SSM に渡しますが、CSC SSM はパケットをスキャンせずに渡します。

CSC SSM の効率を最大限にするには、次のように、**csc** コマンドを実装しているポリシーが使用するクラス マップを設定します。

- サポートされているプロトコルのうち、CSC SSM がスキャンするプロトコルだけを選択します。たとえば、HTTP トラフィックをスキャンしない場合は、サービス ポリシーが HTTP トラフィックを CSC SSM に転送しないようにしてください。
- セキュリティ アプライアンスによって保護されている信頼できるホストを危険にさらす接続だけを選択します。これらは、外部ネットワークまたは信頼できないネットワークから内部ネットワークへの接続です。次の接続をスキャンすることを推奨します。
  - 発信 HTTP 接続。
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの FTP 接続。
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの POP3 接続。
  - 内部メール サーバ宛ての着信 SMTP 接続。

FTP スキャン

CSC SSM は、FTP セッションのプライマリ チャネルが標準ポート（TCP ポート 21）を使用している場合にのみ、FTP ファイル転送のスキャンをサポートします。

FTP インスペクションは、CSC SSM がスキャンする FTP トラフィックに対してイネーブルである必要があります。これは、FTP が、データ転送用にダイナミックに割り当てられたセカンダリ チャネルを使用するためです。セキュリティ アプライアンスは、セカンダリ チャネルに割り当てられるポートを決定し、データ転送の実行を許可するピンホールを開きます。FTP データをスキャンするように CSC SSM が設定されている場合、セキュリティ アプライアンスはデータ トラフィックを CSC SSM に転送します。

FTP インスペクションは、グローバルに、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP インスペクションはグローバルにイネーブルになっています。デフォルトのインスペクション コンフィギュレーションを変更していない場合、CSC SSM による FTP スキャンをイネーブルにするために必要なその他の FTP インスペクション コンフィギュレーションはありません。

FTP インスペクションまたはデフォルトのインスペクション コンフィギュレーションの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

内部ネットワーク上のクライアントから HTTP、FTP、および POP3 接続で外部のネットワークに要求されたトラフィック、および外部のホストから DMZ ネットワーク上のメール サーバに着信する SMTP 接続を CSC SSM に転送するように、セキュリティ アプライアンスを設定する必要があります。内部ネットワークから DMZ ネットワーク上の Web サーバへの HTTP 要求は、スキャンされません。

次のコンフィギュレーションでは、2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部インターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が確実にスキャンされるようにします。csc_out アクセス リストにより、内部から外部インターフェイス上のネットワークへの HTTP 接続が確実にスキャンされるようにもなりますが、このアクセス リストには、内部から DMZ ネットワーク上のサーバへの HTTP 接続を除外する拒否 ACE が含まれています。

2 番めのポリシー csc_in_policy は、外部インターフェイスに適用されます。このポリシーは csc_in アクセス リストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求と HTTP 要求が CSC SSM で確実にスキャンされるようにします。HTTP 要求をスキャンすることで、Web サーバは HTTP ファイルのアップロードから保護されます。

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

（注） FTP により転送されたファイルを CSC SSM がスキャンするには、FTP インスペクションがイネーブルである必要があります。FTP インスペクションは、デフォルトでイネーブルになっています。

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類のクラス マップを指定します。
class-map	ポリシー マップで使用するトラフィック分類マップを作成します。
match port	宛先ポートを使用してトラフィックを照合します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。

csd enable

管理およびリモート ユーザ アクセス用に Cisco Secure Desktop をイネーブルにするには、webvpn コンフィギュレーション モードで **csd enable** コマンドを使用します。Cisco Secure Desktop をディセーブルにするには、このコマンドの **no** 形式を使用します。

csd enable

no csd enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

csd enable コマンドは、次の処理を実行します。

1. 以前の **csd image** *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。
4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. Cisco Secure Desktop をイネーブルにします。

show webvpn csd コマンドを入力して、Cisco Secure Desktop がイネーブルであるかどうかを確認できます。

csd enable コマンドを入力する前に、実行コンフィギュレーション内に **csd image** *path* コマンドが存在する必要があります。

no csd enable コマンドは、実行コンフィギュレーションで Cisco Secure Desktop をディセーブルにします。Cisco Secure Desktop がディセーブルの場合、ユーザは Cisco Secure Desktop Manager にアクセスできず、リモート ユーザは Cisco Secure Desktop を使用できません。

data.xml ファイルを転送または交換する場合は、このファイルを実行コンフィギュレーションにロードするために、Cisco Secure Desktop をいったんディセーブルにしてからイネーブルにします。

例

次に、Cisco Secure Desktop イメージのステータスを表示し、Cisco Secure Desktop イメージをイネーブルにするためのコマンドの使用例を示します。

```
hostname(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	Cisco Secure Desktop がイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd image	コマンドで指定された Cisco Secure Desktop イメージを、パスで指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

csd image

Cisco Secure Desktop 配布パッケージを検証して、実行コンフィギュレーションに追加するには、Cisco Secure Desktop を効率的にインストールし、webvpn コンフィギュレーション モードで **csd image** コマンドを使用します。CSD 配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

csd image *path*

no csd image [*path*]

構文の説明

path	Cisco Secure Desktop パッケージのパスおよびファイル名を 255 文字以内で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、**show webvpn csd** コマンドを入力して、Cisco Secure Desktop イメージがイネーブルであるかどうかを判断します。CLI は、現在インストールされている Cisco Secure Desktop イメージがイネーブルである場合、そのバージョンを示します。

http://www.cisco.com/cisco/software/navigator.html から新しい Cisco Secure Desktop イメージをコンピュータにダウンロードし、フラッシュ ドライブに転送してから、**csd image** コマンドを使用して、イメージをインストールするか、または既存のイメージをアップグレードします。ダウンロードする場合、使用しているセキュリティ アプライアンスに合ったファイルを必ず取得してください。ファイルの形式は、**securedesktop_asa_**<*n*>**_**<*n*>***.pkg** です。

no csd image を入力すると、Cisco Secure Desktop Manager への管理アクセスと、Cisco Secure Desktop へのリモート ユーザ アクセスの両方が削除されます。このコマンドを入力しても、セキュリティ アプライアンスは、Cisco Secure Desktop ソフトウェアおよびフラッシュ ドライブ上の Cisco Secure Desktop コンフィギュレーションに対してどのような変更も行いません。

（注） 次回のセキュリティ アプライアンスのリブート時に Cisco Secure Desktop を確実に使用できるようにするために、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例

次に、現在の Cisco Secure Desktop 配布パッケージを表示し、フラッシュ ファイル システムの内容を表示して、新しいバージョンにアップグレードするためのコマンドの使用例を示します。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
hostname(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	Cisco Secure Desktop がイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd enable	管理およびリモート ユーザ アクセス用に Cisco Secure Desktop をイネーブルにします。

ctl

証明書信頼リスト プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールするには、CTL プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ctl install

no ctl instal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、イネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL プロバイダー コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、CTL ファイルのエントリに対するトラストポイントをインストールするには、CTL プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。このコマンドでインストールされたトラストポイントの名前には「_internal_CTL_<ctl_name>」というプレフィックスが付いています。このコマンドはオプションであり、デフォルトでイネーブルになっています。

このコマンドがディセーブルの場合は、**crypto ca trustpoint** コマンドと **crypto ca certificate chain** コマンドを使用して、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

ctl-file（グローバル）

電話プロキシ用に作成するための CTL インスタンス、またはフラッシュ メモリに格納されている CTL ファイルを解析するための CTL インスタンスを指定するには、グローバル コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタンスを削除するには、このコマンドの **no** 形式を使用します。

ctl-file *ctl_name* **noconfirm**

no ctl-file *ctl_name* **noconfirm**

構文の説明

ctl_name	CTL インスタンスの名前を指定します。
noconfirm	（任意）**no** コマンドとともに使用して、CTL ファイルが削除されたときにトラストポイントの削除に関する警告がセキュリティ アプライアンスのコンソールに表示されないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

LSC プロビジョニングが必要な電話をユーザが所有している場合は、**ctl-file** コマンドを使用して CTL ファイル インスタンスを設定するときに、CAPF 証明書を CUMC から ASA にインポートする必要もあります。『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

（注） CTL ファイルを作成するには、ctl ファイル コンフィギュレーション モードで **no shutdown** コマンドを使用します。CTL ファイルのエントリを変更したり CTL ファイルにエントリを追加したりするには、または CTL ファイルを削除するには、**shutdown** コマンドを使用します。

このコマンドの **no** 形式を使用すると、CTL ファイル、および電話プロキシによって内部的に作成されたすべての登録済みトラストポイントが削除されます。また、CTL ファイルを削除すると、関連する認証局から受信したすべての証明書が破棄されます。

例

次に、**ctl-file** コマンドを使用して、Phone Proxy 機能用の CTL ファイルを設定する例を示します。

```
hostname(config)# ctl-file myctl
```

関連コマンド

コマンド	説明
ctl-file（Phone-Proxy）	電話プロキシ インスタンスの設定時に使用する CTL ファイルを指定します。
cluster-ctl-file	フラッシュ メモリに格納されている CTL ファイルからトラストポイントをインストールするために、CTL ファイルを解析します。
phone-proxy	Phone Proxy インスタンスを設定します。
record-entry	CTL ファイルの作成に使用するトラストポイントを指定します。
sast	CTL レコードに作成する SAST 証明書の数を指定します。

ctl-file（Phone-Proxy）

電話プロキシの設定時に使用する CTL インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタンスを削除するには、このコマンドの **no** 形式を使用します。

ctl-file *ctl_name*

no ctl-file *ctl_name*

構文の説明

ctl_name	CTL インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**ctl-file** コマンドを使用して、Phone Proxy 機能用の CTL ファイルを設定する例を示します。

```
hostname(config-phone-proxy)# ctl-file myctl
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
phone-proxy	電話プロキシ インスタンスを設定します。

ctl-provider

CTL プロバイダー モードで証明書信頼リスト プロバイダー インスタンスを設定するには、グローバル コンフィギュレーション モードで **ctl-provider** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

構文の説明

ctl_name	CTL プロバイダー インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードを開始して CTL プロバイダー インスタンスを作成するには、**ctl-provider** コマンドを使用します。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
client	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
export	クライアントにエクスポートする証明書を指定します。

コマンド	説明
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

customization

トンネル グループ、グループ、またはユーザに使用するカスタマイゼーションを指定するには、次のモードで **customization** コマンドを使用します。

トンネル グループ webvpn 属性コンフィギュレーション モードと webvpn コンフィギュレーション モードの場合（グローバル コンフィギュレーション モードからアクセス可能）

customization *name*

no customization *name*

webvpn コンフィギュレーション モードの場合（グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードからアクセス可能）

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

構文の説明

name	適用する WebVPN カスタマイゼーションの名前を指定します。
none	グループまたはユーザのカスタマイゼーションをディセーブルにし、デフォルトの WebVPN ページを表示します。
value *name*	グループ ポリシーまたはユーザに適用するカスタマイゼーションの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	•	—	•	—	—
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

トンネル グループ webvpn 属性コンフィギュレーション モードで **customization** コマンドを入力する前に、webvpn コンフィギュレーション モードで **customization** コマンドを使用してカスタマイゼーションの名前を付け、設定する必要があります。

Mode-Dependent コマンド オプション

customization コマンドで使用できるキーワードは、現在のモードによって異なります。グループ ポリシー属性 > webvpn コンフィギュレーション モードおよびユーザ名属性 > webvpn コンフィギュレーション モードでは、追加のキーワード **none** と **value** があります。これらのモードでの完全な構文は、次のとおりです。

[**no**] **customization** {**none** | **value** *name*}

none は、グループまたはユーザのカスタマイゼーションをディセーブルにし、カスタマイゼーションが継承されないようにします。たとえば、ユーザ名属性 > webvpn モードで **customization none** コマンドを入力すると、セキュリティ アプライアンスは、グループ ポリシーやトンネル グループ内の値を検索しません。

name は、グループまたはユーザに適用するカスタマイゼーションの名前です。

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

例

次に、パスワード プロンプトを定義する「123」という名前の WebVPN カスタマイゼーションを最初に確立するコマンド シーケンスの例を示します。この例では、次に「test」という WebVPN トンネル グループを定義し、**customization** コマンドを使用して、「123」という WebVPN カスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization 123
hostname(config-tunnel-webvpn)#
```

次に、「cisco」というカスタマイゼーションを「cisco_sales」というグループ ポリシーに適用する例を示します。グループ ポリシー属性 > webvpn コンフィギュレーション モードでは、**customization** コマンドに追加のコマンド オプション **value** が必要となることに注意してください。

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)#  webvpn
hostname(config-group-webvpn)# customization value cisco
```

関連コマンド

コマンド	説明
clear configure tunnel-group	すべてのトンネル グループのコンフィギュレーションを削除します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

CHAPTER 10

database path コマンド～ debug xml コマンド

database path

ローカル CA サーバ データベースのパスまたは位置を指定するには、CA サーバ コンフィギュレーション モードで **database** コマンドを使用します。フラッシュ メモリへのパスをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

[no] database path *mount-name directory-path*

構文の説明

directory-path	CA ファイルが保存される、マウント ポイント上のディレクトリへのパスを指定します。
mount-name	マウント名を指定します。

デフォルト

デフォルトでは、CA サーバ データベースはフラッシュ メモリに保存されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

データベースに保存されるローカル CA ファイルには、証明書データベース ファイル、ユーザ データベース ファイル、一時 PKCS12 ファイル、および現在の CRL ファイルが含まれます。*mount-name* は、セキュリティ アプライアンスのファイル システムを指定するために使用する **mount** コマンドの *name* 引数と同じです。

（注） これらの CA ファイルは内部保存ファイルです。変更しないでください。

例

次に、CA データベースのマウント ポイントを cifs_share と定義する例を示します。また、マウント ポイント上のデータベース ファイル ディレクトリを ca_dir/files_dir と定義しています。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# database path cifs_share ca_dir/files_dir/
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	ローカル CA の設定および管理が可能な CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供します。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報をディスクに書き込みます。
debug crypto ca server	ユーザがローカル CA サーバを設定する場合にデバッグ メッセージを表示します。
mount	Common Internet File System（CIFS; 共通インターネット ファイル システム）および File Transfer Protocol File Systems（FTPFS; ファイル転送プロトコル ファイル システム）の一方または両方を、セキュリティ アプライアンスがアクセスできるようにします。
show crypto ca server	セキュリティ アプライアンスの CA コンフィギュレーションの特性を表示します。
show crypto ca server cert-db	CA サーバが発行する証明書を表示します。

ddns (DDNS-update-method)

DDNS 更新方式のタイプを指定するには、DDNS 更新方式モードで **ddns** コマンドを使用します。実行コンフィギュレーションから更新方式タイプを削除するには、このコマンドの **no** 形式を使用します。

ddns [**both**]

no ddns [**both**]

構文の説明

both	（任意）DNS A と PTR の両方の Resource Record（RR; リソース レコード）の更新を指定します。

デフォルト

A RR のみ更新します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DDNS 更新方式	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

Dynamic DNS（DDNS; ダイナミック DNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングを更新します。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

次の 2 つのタイプの Resource Record（RR; リソース レコード）に、名前マッピングおよびアドレスマッピングが含まれます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

DDNS 更新方式コンフィギュレーション モードで **ddns** コマンドを発行するとき、更新を A RR に対してのみ行うか、A RR と PTR RR の両方に対して行うかを定義します。

例

次に、ddns-2 という名前の DDNS 更新方式に対し A と PTR の両方の RR の更新を設定する例を示します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

関連コマンド

コマンド	説明
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update（インターフェイス コンフィギュレーション）

Dynamic DNS（DDNS; ダイナミック DNS）更新方式を、セキュリティ アプライアンス インターフェイスまたは更新ホスト名に関連付けるには、インターフェイス コンフィギュレーション モードで **ddns update** コマンドを使用します。DDNS 更新方式とインターフェイスまたはホスト名とのアソシエーションを、実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

構文の説明

hostname	コマンド文字列内の後続の語をホスト名として指定します。
hostname	更新で使用するホスト名を指定します。
method-name	設定するインターフェイスとのアソシエーションの方式名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS 更新方式を定義した後、DDNS 更新をトリガーするために、その DDNS 更新方式をセキュリティ アプライアンス インターフェイスに関連付ける必要があります。

ホスト名は、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）またはホスト名のみを指定できます。ホスト名のみ指定した場合、セキュリティ アプライアンスは、ドメイン名をホスト名に追加して FQDN を作成します。

例

次に、インターフェイス GigabitEthernet0/2 に ddns-2 という名前の DDNS 更新方式およびホスト名 hostname1.example.com を関連付ける例を示します。

```
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname hostname1.example.com
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update method（グローバル コンフィギュレーション モード）

DNS Resource Record（RR; リソース レコード）をダイナミックに更新するための方式を作成するには、グローバル コンフィギュレーション モードで **ddns update method** コマンドを使用します。実行コンフィギュレーションから Dynamic DNS（DDNS; ダイナミック DNS）更新方式を削除するには、このコマンドの **no** 形式を使用します。

ddns update method *name*

no ddns update method *name*

構文の説明

name	ダイナミックに DNS レコードを更新するための方式の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。**ddns update method** コマンドで設定する更新方式により、ダイナミック DNS 更新の実行方法および実行頻度が決まります。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

次の 2 つのタイプの Resource Record（RR; リソース レコード）に、名前マッピングおよびアドレス マッピングが含まれます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

（注） **ddns update method** を実行する前に、インターフェイスでドメイン ルックアップをイネーブルにした状態で、**dns** コマンドを使用して到達可能なデフォルト DNS サーバを設定する必要があります。

例

次に、ddns-2 という名前の DDNS 更新方式を設定する例を示します。

```
hostname(config)# ddns update method ddns-2
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

debug aaa

AAA のデバッグ メッセージを表示するには、特権 EXEC モードで **debug aaa** コマンドを使用します。AAA メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug aaa [**accounting** | **authentication** | **authorization** | **common** | **internal** | **vpn** [*level*]]

no debug aaa

構文の説明

accounting	（任意）アカウンティングのデバッグ メッセージのみ表示します。
authentication	（任意）認証のデバッグ メッセージのみ表示します。
authorization	（任意）認可のデバッグ メッセージのみ表示します。
common	（任意）AAA 機能内の各種状態に関するデバッグ メッセージを表示します。
internal	（任意）ローカル データベースがサポートする AAA 機能に関するデバッグ メッセージのみ表示します。
level	（任意）デバッグ レベルを指定します。**vpn** キーワードを指定した場合に限り有効です。
vpn	（任意）VPN 関連の AAA 機能のデバッグ メッセージのみ表示します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは変更され、新しいキーワードが追加されました。

使用上のガイドライン

debug aaa コマンドは、AAA アクティビティに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、ローカル データベースがサポートする AAA 機能のデバッグをイネーブルにする例を示します。

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

関連コマンド

コマンド	説明
show running-config aaa	AAA に関連する実行コンフィギュレーションを表示します。

debug appfw

アプリケーション インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug appfw** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

構文の説明

chunk	（任意）チャンク転送エンコード パケットの処理に関する実行時情報を表示します。
event	（任意）パケット インスペクション イベントに関するデバッグ情報を表示します。
eventverb	（任意）イベントへの応答でセキュリティ アプライアンスが実行したアクションを表示します。
regex	（任意）定義済みシグニチャを使用したマッチング パターンに関する情報を表示します。

デフォルト

デフォルトでは、すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug appfw コマンドは、HTTP アプリケーション インスペクションに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug appfw
```

関連コマンド

コマンド	説明
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。

debug arp

ARP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp** コマンドを使用します。ARP のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp

no debug arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、ARP のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug arp
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
show arp statistics	ARP 統計情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug arp-inspection

ARP インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp-inspection** コマンドを使用します。ARP インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp-inspection

no debug arp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、ARP インスペクションのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug arp-inspection
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show debug	イネーブルなデバッガをすべて表示します。

debug asdm history

ASDM のデバッグ情報を表示するには、特権 EXEC モードで **debug asdm history** コマンドを使用します。

debug asdm history *level*

構文の説明

level	（任意）デバッグ レベルを指定します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**debug pdm history** コマンドから **debug asdm history** コマンドに変更されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、ASDM のレベル 1 デバッグをイネーブルにする例を示します。

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

debug context

セキュリティ コンテキストを追加または削除するときにデバッグ メッセージを表示するには、特権 EXEC モードで **debug context** コマンドを使用します。コンテキストのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug context [*level*]

no debug context [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、コンテキスト管理のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug context
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキスト情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug cplane

SSM に内部接続するコントロール プレーンに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug cplane** コマンドを使用します。コントロール プレーンに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug cplane [*level*]

no debug cplane [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、コントロール プレーンのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug cplane
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。

コマンド	説明
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug crypto ca

（CA で使用される）PKI アクティビティのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto ca** コマンドを使用します。PKI のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ca [**messages** | **transactions**] [*level*]

no debug crypto ca [**messages** | **transactions**] [*level*]

構文の説明

messages	（任意）PKI 入力および出力メッセージのデバッグ メッセージのみ表示します。
transactions	（任意）PKI トランザクションのデバッグ メッセージのみ表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。レベル 1（デフォルト）では、エラーが発生した場合に限りメッセージが表示されます。レベル 2 では、警告が表示されます。レベル 3 では、情報メッセージが表示されます。レベル 4 以上では、トラブルシューティングのための追加メッセージが表示されます。

デフォルト

デフォルトでは、このコマンドはすべてのデバッグ メッセージを表示します。デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、PKI のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto ca
```

関連コマンド

コマンド	説明
debug crypto engine	暗号化エンジンのデバッグ メッセージを表示します。
debug crypto ipsec	IPSec のデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP のデバッグ メッセージを表示します。

debug crypto ca server

ローカル CA サーバのデバッグ メッセージのレベルを設定し、関連するデバッグ メッセージのリスト表示を開始するには、CA サーバ コンフィギュレーション モードで **debug crypto ca server** コマンドを使用します。すべてのデバッグ メッセージのリスト表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ca server [*level*]

no debug crypto ca server [*level*]

構文の説明

level	表示するデバッグ メッセージのレベルを設定します。指定できる値の範囲は 1 ～ 255 です。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。レベル 5 以上は raw データ ダンプ用に予約されており、デバッグ出力が非常に多くなるため、通常のデバッグ時には使用しないでください。

例

次の例では、デバッグ レベルを 3 に設定しています。

```
hostname(config-ca-server)# debug crypto ca server 3
hostname(config-ca-server)#
```

次に、すべてのデバッグをオフにする例を示します。

```
hostname(config-ca-server)# no debug crypto ca server
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める Certificate Revocation List（CRL; 証明書失効リスト）Distribution Point（CDP; 証明書失効リスト分散ポイント）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
database path	ローカル CA サーバ データベースのパスまたは位置を指定します。
show crypto ca server	ASCII テキスト形式でセキュリティ アプライアンスの認証局のコンフィギュレーションの特性を表示します。
show crypto ca server certificate	base64 形式でローカル CA コンフィギュレーションを表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

debug crypto condition

指定した条件に基づき IPSec および ISAKMP のデバッグ メッセージをフィルタリングするには、特権 EXEC モードで **debug crypto condition** コマンドを使用します。他の条件に影響を与えずに単一のフィルタリング条件をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug crypto condition [[peer [address *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [spi *spi*] | [**reset**]

[no] debug crypto condition [[peer [address *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [**spi** *spi*] | [**reset**]

構文の説明

group *group_name*	使用するグループおよびクライアント グループ名を指定します。
peer *peer_addr*	IPSec ピアおよびその IP アドレスを指定します。
reset	すべてのフィルタリング条件をクリアし、フィルタリングをディセーブルにします。
spi *spi*	IPSec SPI を指定します。
subnet *subnet_mask*	指定した IP アドレスに関連するサブネットおよびサブネット マスクを指定します。
user *user_name*	使用するクライアントおよびクライアント ユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug crypto condition コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、ネットワーク 10.1.1.0 およびピア 10.2.2.2 のフィルタを設定する例を示します。

```
hostname# debug crypto condition peer address 10.1.1.0 subnet 255.255.255.0
hostname# debug crypto condition peer address 10.2.2.2
```

次に、ユーザ「example_user」のフィルタを設定する例を示します。

```
hostname# debug crypto condition user example_user
```

次に、デバッグ フィルタをクリアする例を示します。

```
hostname# debug crypto condition reset
```

関連コマンド

コマンド	説明
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto condition error

IPSec および ISAKMP のデバッグ メッセージが設定済みのフィルタに一致するかどうかに関係なく、それらのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto condition error** コマンドを使用します。IPSec および ISAKMP のデバッグ メッセージが設定済みのフィルタに一致するかどうかに関係なく、それらのデバッグ メッセージを表示しないようにするには、このコマンドの **no** 形式を使用します。

debug crypto condition error [[ipsec | isakmp]

[no] debug crypto condition error [ipsec | isakmp]

構文の説明

ipsec	IPSec デバッグ メッセージ システムを指定します。
isakmp	ISAKMP デバッグ メッセージ システムを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug crypto condition error コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、フィルタリング条件が指定されているかどうかに関係なく、IPSec メッセージが表示されるように設定する例を示します。

```
hostname# debug crypto condition error ipsec
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。

コマンド	説明
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto condition unmatched

フィルタリングのための十分なコンテキスト情報を含まない IPSec および ISAKMP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto condition unmatched** コマンドを使用します。十分なコンテキスト情報を含まない IPSec および ISAKMP のデバッグ メッセージをフィルタリングするには、このコマンドの **no** 形式を使用します。

debug crypto condition unmatched [[ipsec | isakmp]

[no] debug crypto condition unmatched [**ipsec | isakmp]**

構文の説明

ipsec	IPSec デバッグ メッセージ システムを指定します。
isakmp	ISAKMP デバッグ メッセージ システムを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug crypto condition unmatched コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、十分なコンテキストを含まない IPSec メッセージが表示されるようにフィルタを設定する例を示します。

```
hostname# debug crypto condition unmatched ipsec
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。

コマンド	説明
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto engine

クリプト エンジンのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto engine** コマンドを使用します。クリプト エンジンのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto engine [*level*]

no debug crypto engine [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、クリプト エンジンのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto engine
```

関連コマンド

コマンド	説明
debug crypto ca	CA のデバッグ メッセージを表示します。
debug crypto ipsec	IPSec のデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP のデバッグ メッセージを表示します。

debug crypto ipsec

IPSec のデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto ipsec** コマンドを使用します。IPSec のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、IPSec のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto ipsec
```

関連コマンド

コマンド	説明
debug crypto ca	CA のデバッグ メッセージを表示します。
debug crypto engine	暗号化エンジンのデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP のデバッグ メッセージを表示します。

debug crypto isakmp

ISAKMP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto isakmp** コマンドを使用します。ISAKMP のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto isakmp [**timers**] [*level*]

no debug crypto isakmp [**timers**] [*level*]

構文の説明

timers	（任意）ISAKMP タイマー失効のデバッグ メッセージを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。レベル 1（デフォルト）では、エラーが発生した場合に限りメッセージが表示されます。レベル 2 ～ 7 では、追加情報が表示されます。レベル 254 では、ヒト可読形式で復号化 ISAKMP パケットが表示されます。レベル 255 では、復号化 ISAKMP パケットの 16 進数ダンプが表示されます。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、ISAKMP のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto isakmp
```

関連コマンド

コマンド	説明
debug crypto ca	CA のデバッグ メッセージを表示します。

コマンド	説明
debug crypto engine	暗号化エンジンのデバッグ メッセージを表示します。
debug crypto ipsec	IPSec のデバッグ メッセージを表示します。

debug ctiqbe

CTIQBE アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctiqbe** コマンドを使用します。CTIQBE アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug ctiqbe** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、CTIQBE アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ctiqbe
```

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。

コマンド	説明
show ctiqbe	セキュリティ アプライアンスを通じて確立された CTIQBE セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug ctl-provider

証明書信頼リスト プロバイダーのデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctl-provider** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ctl-provider [**errors** | **events** | **parser**]

no debug ctl-provider [**errors** | **events** | **parser**]

構文の説明

errors	CTL プロバイダー エラー デバッグを指定します。
events	CTL プロバイダー イベント デバッグを指定します。
parser	CTL プロバイダー パーサー デバッグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、CTL プロバイダーのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ctl-provider
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。

debug dap

ダイナミック アクセス ポリシー イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug dap** コマンドを使用します。DAP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dap {errors | trace}

no debug dap [errors | trace]

構文の説明

errors	DAP 処理エラーを指定します。
trace	DAP 機能トレースを指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
hostname # debug dap trace
hostname #
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。

debug ddns

DDNS のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ddns** コマンドを使用します。デバッグ メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ddns

no debug ddns

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug ddns コマンドは、DDNS に関する詳細情報を表示します。**undebug ddns** は、**no debug ddns** コマンドと同様に、DDNS デバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DDNS デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ddns
debug ddns enabled at level 1
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。

コマンド	説明
ddns update（インターフェイス コンフィギュレーション モード）	DDNS アップデート方式をセキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

debug dhcpc

DHCP クライアントのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpc** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpc {**detail** | **packet** | **error**} [*level*]

no debug dhcpc {**detail** | **packet** | **error**} [*level*]

構文の説明

detail	DHCP クライアントに関連する詳細イベント情報を表示します。
error	DHCP クライアントに関連するエラー メッセージを表示します。
level	（任意）デバッグ レベルを指定します。有効な値の範囲は 1 ～ 255 です。
packet	DHCP クライアントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

DHCP クライアントのデバッグ情報を表示します。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP クライアントのデバッグをイネーブルにするためのコマンドの使用例を示します。

```
hostname# debug dhcpc detail 5
debug dhcpc detail enabled at level 5
```

関連コマンド

コマンド	説明
show ip address dhcp	インターフェイスの DHCP リースに関する詳細情報を表示します。
show running-config interface	指定したインターフェイスの実行コンフィギュレーションを表示します。

debug dhcpd

DHCP サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpd** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpd {**event** | **packet**} [*level*]

no debug dhcpd {**event** | **packet**} [*level*]

構文の説明

event	DHCP サーバに関連するイベント情報を表示します。
level	（任意）デバッグ レベルを指定します。有効な値の範囲は 1 ～ 255 です。
packet	DHCP サーバに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug dhcpd event コマンドは、DHCP サーバに関するイベント情報を表示します。**debug dhcpd packet** コマンドは、DHCP サーバに関するパケット情報を表示します。

デバッグをディセーブルにするには、**debug dhcpd** コマンドの **no** 形式を使用します。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP イベントのデバッグをイネーブルにする例を示します。

```
hostname# debug dhcpd event
debug dhcpd event enabled at level 1
```

関連コマンド

コマンド	説明
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

debug dhcpd ddns

DHCP DDNS のデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpd ddns** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpd ddns [*level*]

no debug dhcpd ddns [*level*]

構文の説明

level	（任意）デバッグ レベルを指定します。有効値の範囲は、1 ～ 255 です。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug dhcpd ddns コマンドは、DHCP および DDNS に関する詳細情報を表示します。**undebug dhcpd ddns** コマンドは、**no debug dhcpd ddns** コマンドと同様に、DHCP と DDNS のデバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP DDNS のデバッグをイネーブルにする例を示します。

```
hostname# debug dhcpd ddns
debug dhcpd ddns enabled at level 1
```

関連コマンド

コマンド	説明
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。
show running-config ddns	実行コンフィギュレーションの DDNS 更新方式を表示します。

debug dhcprelay

DHCP リレー サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpreleay** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcprelay {**event** | **packet** | **error**} [*level*]

no debug dhcprelay {**event** | **packet** | **error**} [*level*]

構文の説明

error	DHCP リレー エージェントに関連するエラー メッセージを表示します。
event	DHCP リレー エージェントに関連するイベント情報を表示します。
level	（任意）デバッグ レベルを指定します。有効な値の範囲は 1 ～ 255 です。
packet	DHCP リレー エージェントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP リレー エージェントのエラー メッセージのデバッグをイネーブルにする方法の例を示します。

```
hostname# debug dhcprelay error
debug dhcprelay error enabled at level 1
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェントの統計カウンタをクリアします。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

debug disk

ファイル システムのデバッグ情報を表示するには、特権 EXEC モードで **debug disk** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug disk {**file** | **file-verbose** | **filesystem**} [*level*]

no debug disk {**file** | **file-verbose** | **filesystem**}

構文の説明

file	ファイルレベルのディスク デバッグ メッセージをイネーブルにします。
file-verbose	ファイル レベルでの詳細なディスクのデバッグ メッセージをイネーブルにします。
filesystem	ファイル システムのデバッグ メッセージをイネーブルにします。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、ファイルレベルのディスク デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドで、ファイルレベルのディスク デバッグ メッセージがイネーブルになっていることを確認できます。**dir** コマンドにより、いくつかのデバッグ メッセージが発生します。

```
hostname# debug disk file
debug disk file enabled at level 1
hostname# show debug
```

```
debug vpn-sessiondb  enabled at level 1
hostname# dir
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3

Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0

4      -rw-  5124096     14:42:27 Apr 04 2005  cdisk.binIFS: Opened: file flash:/ as fd 3

9      -rw-  5919340     14:53:39 Apr 04 2005  ASDMIFS: Getdent: fd 3

11     drw-  0           15:18:56 Apr 21 2005  syslog
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3

16128000 bytes total (5047296 bytes free)
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug dns

DNS のデバッグ メッセージを表示するには、特権 EXEC モードで **debug dns** コマンドを使用します。DNS のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug dns [**resolver** | **all**] [*level*]

no debug dns [**resolver** | **all**] [*level*]

構文の説明

all	（デフォルト）DNS キャッシュに関するメッセージを含むすべてのメッセージを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。
resolver	（任意）DNS リゾルバ メッセージのみ表示します。

デフォルト

デフォルトの level は 1 です。キーワードを指定しない場合、セキュリティ アプライアンスによりすべてのメッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、DNS のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug dns
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect dns	DNS アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug eap

EAP イベントのロギングをイネーブルにして NAC メッセージをデバッグするには、特権 EXEC モードで **debug eap** コマンドを使用します。EAP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eap {**all** | **errors** | **events** | **packets** | **sm**}

no debug eap [**all** | **errors** | **events** | **packets** | **sm**]

構文の説明

all	すべての EAP 情報に関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAP パケット エラーのロギングをイネーブルにします。
events	EAP セッション イベントのロギングをイネーブルにします。
packets	EAP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAP ステート マシン情報に関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、EAP セッション状態の変化および EAP ステータス クエリー イベントを記録し、16 進数形式で EAP およびパケット コンテンツの完全レコードを生成します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての EAP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug eap events
hostname#
```

次に、すべての EAP デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug eap all
hostname#
```

次に、すべての EAP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug eap
hostname#
```

関連コマンド

コマンド	説明
debug eou	NAC メッセージングをデバッグするための EAPoUDP イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つ以上の NAC セッションに割り当てられているリソースを消去し、セッションごとに、新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC セッションの即時ポスチャ確認を強制実行します。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug eigrp fsm

DUAL 有限状態マシンのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp fsm** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eigrp fsm

no debug eigrp fsm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、EIGRP フィジブル サクセサ アクティビティをモニタし、ルート更新がルーティング プロセスによりインストールされているかどうか、および削除されているかどうかを確認できます。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp fsm** コマンドの出力例を示します。

```
hostname# debug eigrp fsm

DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 4294967295
found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

最初の行の DUAL は Diffusing Update Algorithm（DUAL; 拡散更新アルゴリズム）の略語です。DUAL は、ルーティングを決定する EIGRP 内の基本メカニズムです。次の 3 つのフィールドは、宛先ネットワークのインターネット アドレスとマスク、および更新を受信したときに経由したアドレスです。metric フィールドは、ルーティング データベルに保存されているメトリック、および情報を送信するネイバーがアドバイタイズしたメトリックを表します。「Metric... inaccessible」という語句が表示された場合、通常、隣接ルータが宛先へのルートを失ったこと、または宛先がホールドダウン状態であることを示します。

次の出力では、EIGRP は、宛先のフィジブル サクセサを検出しようとしています。フィジブル サクセサは、DUAL ループ回避方式の一部です。FD フィールドには、追加のループ回避状態情報が含まれます。RD フィールドはレポートされるディスタンスで、これは更新パケット、クエリー パケット、または応答パケットで使用されるメトリックです。

「not found」メッセージを含むインデントされた行は、192.168.4.0 についてフィジブル サクセサが検出されなかったことを示し、EIGRP が拡散の計算を開始する必要があることを示します。これは、EIGRP が、192.164.4.0 への代替パスを検出するために、ネットワークのアクティブ プローブを開始すること（宛先 192.168.4.0 に関するクエリー パケットを送信すること）を意味します。

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

次の出力は、ルート DUAL がルーティング テーブルに正常にインストールされたことを示します。

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

次の出力は、宛先へのルートが検出されなかったこと、およびルート情報がトポロジ テーブルから削除されることを示します。

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp topology	EIGRP トポロジ テーブルを表示します。

debug eigrp neighbors

EIGRP により検出されたネイバーのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp neighbors** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eigrp neighbors [**siatimer** | **static**]

no debug eigrp neighbors [**siatimer** | **static**]

構文の説明

siatimer	（任意）アクティブ メッセージの EIGRP スタックを表示します。
static	（任意）EIGRP スタティック ネイバー メッセージを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp neighbors static** コマンドの出力例を示します。この例では、スタティック ネイバーの追加と削除、および対応するデバッグ メッセージが示されています。

```
hostname# debug eigrp neighbors static

EIGRP Static Neighbors debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Multicast Hello is disabled on Ethernet0/0!
```

```
EIGRP: Add new static nbr 10.86.194.3 to AS 100 Ethernet0/0

hostname(config-router)# no neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Static nbr 10.86.194.3 not in AS 100 Ethernet0/0 dynamic list
EIGRP: Delete static nbr 10.86.194.3 from AS 100 Ethernet0/0
EIGRP: Multicast Hello is enabled on Ethernet0/0!

hostname(config-router)# no debug eigrp neighbors static

EIGRP Static Neighbors debugging is off
```

関連コマンド

コマンド	説明
neighbor	EIGRP ネイバーを定義します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

debug eigrp packets

EIGRP パケットのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp packets** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

no debug eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

構文の説明

ack	（任意）デバッグ出力を EIGRP ACK パケットに制限します。
hello	（任意）デバッグ出力を EIGRP hello パケットに制限します。
probe	（任意）デバッグ出力を EIGRP プローブ パケットに制限します。
query	（任意）デバッグ出力を EIGRP クエリー パケットに制限します。
reply	（任意）デバッグ出力を EIGRP 応答パケットに制限します。
request	（任意）デバッグ出力を EIGRP 要求パケットに制限します。
retry	（任意）デバッグ出力を EIGRP 再試行パケットに制限します。
SIAquery	（任意）デバッグ出力をアクティブ クエリー パケットの EIGRP スタックに制限します。
SIAreply	（任意）デバッグ出力をアクティブ応答パケットの EIGRP スタックに制限します。
stub	（任意）デバッグ出力を EIGRP スタブ ルーティング パケットに制限します。
terse	（任意）hello パケット以外のすべての EIGRP パケットを表示します。
update	（任意）デバッグ出力を EIGRP 更新パケットに制限します。
verbose	（任意）すべてのパケット デバッグ メッセージを出力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

単一のコマンドで複数のパケット タイプを指定できます。以下に例を示します。

```
debug eigrp packets query reply
```

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp packets** コマンドの出力例を示します。

```
hostname# debug eigrp packets

EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x0, Seq 2, Ack 0
```

この出力は、EIGRP パケットの送信と受信を示しています。EIGRP の信頼できるトランスポート アルゴリズムで使用されるシーケンス番号および確認応答番号が出力に表示されています。該当する場合、隣接ルータのネットワーク層アドレスも含まれます。

関連コマンド

コマンド	説明
show eigrp traffic	送受信された EIGRP パケットの数を表示します。

debug eigrp transmit

EIGRP により送信された送信メッセージを表示するには、特権 EXEC モードで **debug eigrp transmit** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

構文の説明

ack	（任意）システムが送信した Acknowledgment（ACK; 確認応答）メッセージの情報。
build	（任意）構築情報メッセージ（トポロジ テーブルが正常に構築されたこと、または構築できなかったことを示すメッセージ）。
detail	（任意）デバッグ出力の追加詳細。
link	（任意）トポロジ テーブル リンクリストの管理に関する情報。
packetize	（任意）パケット化イベントに関する情報。
peerdown	（任意）ピアがダウンした場合のパケット生成への影響に関する情報。
sia	（任意）Stuck-in-active メッセージ。
startup	（任意）送信されたピア起動パケットおよび初期化パケットに関する情報。
strange	（任意）パケット処理に関連する通常外イベント。

デフォルト

送信イベントを少なくとも 1 つ指定していない場合、すべての送信イベントがデバッグ出力に表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

単一のコマンドで複数の送信イベントを指定できます。以下に例を示します。

```
hostname# debug eigrp ack build link
```

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してく

ださい。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp transmit** コマンドの出力例を示します。この例では、**network** コマンドの入力、および生成された送信イベント デバッグ メッセージが示されています。

```
hostname# debug eigrp transmit

EIGRP Transmission Events debugging is on

    (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

hostname# configure terminal
hostname(config)# router eigrp 100
hostname(config-router)# network 10.86.194.0 255.255.255.0

DNDB UPDATE 10.86.194.0 255.255.255.0, serno 0 to 1, refcount 0

hostname(config-router)# no debug eigrp transmit

EIGRP Transmission Events debugging is off
```

関連コマンド

コマンド	説明
show eigrp traffic	送受信された EIGRP パケットの数を表示します。

debug eigrp user-interface

EIGRP ユーザ イベントのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp user-interface** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eigrp user-interface

no debug eigrp user-interface

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp user-interface** コマンドの出力例を示します。管理者が EIGRP コンフィギュレーションから **passive-interface** コマンドを削除することで出力が生成されています。

```
hostname# debug eigrp user-interface

EIGRP UI Events debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# no passive-interface inside

CSB2AF: FOUND (AS=100, Name=, VRF=0, AFI=ipv4)

hostname(config-router)# no debug eigrp user-interface
```

```
EIGRP UI Events debugging is off
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
show running-config eigrp	実行コンフィギュレーションの EIGRP コマンドを表示します。

debug entity

MIB のデバッグ情報を表示するには、特権 EXEC モードで **debug entity** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug entity [*level*]

no debug entity

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MIB のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、MIB のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug entity
debug entity  enabled at level 1
hostname# show debug
debug entity  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug eou

EAPoUDP イベントのロギングをイネーブルにして、NAC メッセージをデバッグするには、特権 EXEC モードで **debug eou** コマンドを使用します。EAPoUDP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eou {**all** | **eap** | **errors** | **events** | **packets** | **sm**}

no debug eou [**all** | **eap** | **errors** | **events** | **packets** | **sm**]

構文の説明

all	すべての EAPoUDP 情報に関するデバッグ メッセージのロギングをイネーブルします。
eap	EAPoUDP パケットに関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAPoUDP パケット エラーのロギングをイネーブルにします。
events	EAPoUDP セッション イベントのロギングをイネーブルにします。
packets	EAPoUDP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAPoUDP ステート マシン情報に関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、EAPoUDP セッション状態の変化およびタイマー イベントを記録し、16 進数形式で EAPoUDP ヘッダーとパケット コンテンツの完全レコードを生成します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての EAPoUDP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug eou events
hostname#
```

次に、すべての EAPoUDP デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug eou all
hostname#
```

次に、すべての EAPoUDP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug eou
hostname#
```

関連コマンド

コマンド	説明
debug eap	EAP イベントのロギングをイネーブルにして、NAC メッセージをデバッグします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つ以上の NAC セッションに割り当てられているリソースを消去し、セッションごとに、新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC セッションの即時ポスチャ確認を強制実行します。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug esmtp

SMTP/ESMTP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug esmtp** コマンドを使用します。SMTP/ESMTP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug esmtp [*level*]

no debug esmtp [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug esmtp** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、SMTP/ESMTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug esmtp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。

コマンド	説明
inspect esmtp	ESMTP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SMTP を含む各種接続タイプの接続状態を表示します。

debug fixup

アプリケーション インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug fixup** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fixup

no debug fixup

デフォルト

デフォルトでは、すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug fixup コマンドは、アプリケーション インスペクションに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect *protocol*	特定プロトコルについてアプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

debug fover

フェールオーバーのデバッグ情報を表示するには、特権 EXEC モードで **debug fover** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fover {**cable** | **cmd-exec** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdmp** | **rxip** | **switch** | **sync** | **tx** | **txdmp** | **txip** | **verify**}

no debug fover {**cable** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdmp** | **rxip** | **switch** | **sync** | **tx** | **txdmp** | **txip** | **verify**}

構文の説明

cable	フェールオーバーの LAN ステータスまたはシリアル ケーブル ステータス。
cmd-exec	**failover exec** コマンドの実行トレース。
fail	フェールオーバーの内部例外。
fmsg	フェールオーバー メッセージ。
ifc	ネットワーク インターフェイス ステータスのトレース。
open	フェールオーバー デバイスのオープン。
rx	フェールオーバー メッセージの受信。
rxdmp	フェールオーバー受信メッセージのダンプ（シリアル コンソールのみ）。
rxip	IP ネットワークのフェールオーバー パケットの受信。
switch	フェールオーバー スイッチング ステータス。
sync	フェールオーバーのコンフィギュレーションまたはコマンドのレプリケーション。
tx	フェールオーバー メッセージの送信。
txdmp	フェールオーバー送信メッセージのダンプ（シリアル コンソールのみ）。
txip	IP ネットワークのフェールオーバー パケットの送信。
verify	フェールオーバー メッセージの確認。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。このコマンドには、追加のデバッグ キーワードが含まれます。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug fover cmd-exec** コマンドの出力例を示します。デバッグをイネーブルにした後、**failover exec** コマンドを入力しています。デバッグ出力の後に、**failover exec** コマンドの結果が表示されています。

```
hostname(config)# debug fover cmd-exec

fover event trace on

hostname(config)# failover exec mate show running-config failover

ci/console: Sending cmd: show runn failovero to peer for execution, seq = 4
ci/console: frep_execv_cmd: replicating exec cmd: show runn failover...
fover_parse: Fover rexec response: seq=4, size=228, data="fail..."
ci/console: Fover rexec waiting at clock tick 2670960
fover_parse: Fover rexec ack: seq = 4, ret_val = 0
ci/console: Fover rexec conteinuer at clock tick: 2671040
ci/console: Fover exec succeeded, seq = 5

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover key *****
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show failover	フェールオーバー コンフィギュレーションおよび動作統計に関する情報を表示します。

debug fsm

FSM デバッグ情報を表示するには、特権 EXEC モードで **debug fsm** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fsm [*level*]

no debug fsm

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、FSM デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、FSM デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug fsm
debug fsm  enabled at level 1
hostname# show debug
debug fsm  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ftp client

FTP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ftp client** コマンドを使用します。FTP のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ftp client [*level*]

no debug ftp client [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug ftp client** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、FTP に対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ftp client
```

関連コマンド

コマンド	説明
copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。

コマンド	説明
ftp mode passive	FTP セッションのモードを設定します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

debug generic

各種のデバッグ情報を表示するには、特権 EXEC モードで **debug generic** コマンドを使用します。各種のデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug generic [*level*]

no debug generic

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、各種のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、各種のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug generic
debug generic  enabled at level 1
hostname# show debug
debug generic  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug gtp

GTP インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug gtp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug gtp {**error** | **event** | **ha** | **parser**}

no debug gtp {**error** | **event** | **ha** | **parser**}

構文の説明

error	GTP メッセージの処理中に発生したエラーのデバッグ情報を表示します。
event	GTP イベントのデバッグ情報を表示します。
ha option	GTP HA イベントのデバッグ情報。
parser	GTP メッセージの解析に関するデバッグ情報を表示します。

デフォルト

デフォルトでは、すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug gtp コマンドは、GTP インスペクションに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグ コマンドをオフにします。

（注） GTP インスペクションには、特別なライセンスが必要です。

例

次に、GTP インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug gtp
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。

コマンド	説明
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションで使用する GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定 GTP マップを表示します。

debug h323

H.323 のデバッグ メッセージを表示するには、特権 EXEC モードで **debug h323** コマンドを使用します。H.323 のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug h323 {h225 | h245 | ras} [asn | event]

no debug h323 {h225 | h245 | ras} [asn | event]

構文の説明

h225	H.225 シグナリングを指定します。
h245	H.245 シグナリングを指定します。
ras	登録、アドミッション、およびステータス プロトコルを指定します。
asn	（任意）デコードされたプロトコル データ ユニット（PDU）の出力を表示します。
event	（任意）シグナリング イベントを表示します。または両方のトレースをオンにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug h323** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、H.225 シグナリングに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug h323 h225
```

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h225	セキュリティ アプライアンスで確立されている H.225 セッションの情報を表示します。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | **h323**	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

debug http

HTTP トラフィックに関する詳細情報を表示するには、特権 EXEC モードで **debug http** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug http [*level*]

no debug http [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

debug http コマンドは、HTTP トラフィックに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、HTTP トラフィックに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug http
```

関連コマンド

コマンド	説明
http	セキュリティ アプライアンスの内部の HTTP サーバにアクセスできるホストを指定します。
http-proxy	HTTP プロキシ サーバを設定します。
http redirect	HTTP トラフィックを HTTPS にリダイレクトします。
http server enable	セキュリティ アプライアンス HTTP サーバをイネーブルにします。

debug http-map

HTTP アプリケーション インスペクション マップのデバッグ メッセージを表示するには、特権 EXEC モードで **debug http-map** コマンドを使用します。HTTP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug http-map

no debug http-map

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug http-map** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、HTTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug http-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	HTTP アプリケーション インスペクションに関する詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

debug icmp

ICMP インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug icmp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug icmp trace [*level*]

no debug icmp trace [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。
trace	ICMP トレース アクティビティに関するデバッグ情報を表示します。

デフォルト

すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

debug icmp コマンドは、ICMP インスペクションに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、ICMP インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
show conn	各種プロトコルおよびセッション タイプの、セキュリティ アプライアンスを通じた接続の状態を表示します。

コマンド	説明
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

debug igmp

IGMP のデバッグ情報を表示するには、特権 EXEC モードで **debug igmp** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug igmp [**group** *group_id* | **interface** *if_name*]

no debug igmp [**group** *group_id* | **interface** *if_name*]

構文の説明

group *group_id*	指定したグループの IGMP デバッグ情報を表示します。
interface *if_name*	指定したインターフェイスの IGMP デバッグ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug igmp** コマンドの出力例を示します。

```
hostname#debug igmp

IGMP debugging is on
IGMP: Received v2 Query on outside from 192.168.3.2
IGMP: Send v2 general Query on dmz
IGMP: Received v2 Query on dmz from 192.168.4.1
IGMP: Send v2 general Query on outside
IGMP: Received v2 Query on outside from 192.168.3.1
IGMP: Send v2 general Query on inside
IGMP: Received v2 Query on inside from 192.168.1.1
IGMP: Received v2 Report on inside from 192.168.1.6 for 224.1.1.1
```

```
IGMP: Updating EXCLUDE group timer for 224.1.1.1
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

debug ils

ILS のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ils** コマンドを使用します。ILS のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ils [*level*]

no debug ils [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug ils** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、ILS アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ils
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect ils	ILS アプリケーション インスペクションをイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug imagemgr

Image Manager のデバッグ情報を表示するには、特権 EXEC モードで **debug imagemgr** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug imagemgr [*level*]

no debug imagemgr

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、Image Manager のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドでは、Image Manager のデバッグ メッセージがイネーブルになっていることを確認できます。

```
hostname# debug imagemgr
debug imagemgr  enabled at level 1
hostname# show debug
debug imagemgr  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug inspect tls-proxy

TLS プロキシ インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug inspect tls-proxy** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

no debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

構文の説明

all	すべての TLS プロキシのデバッグを指定します。
errors	TLS プロキシ エラーのデバッグを指定します。
events	TLS プロキシ イベントのデバッグを指定します。
packets	TLS プロキシ パケットのデバッグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、TLS プロキシのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug inspect tls-proxy
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。

コマンド	説明
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

debug ip eigrp

EIGRP プロトコル パケットのデバッグ情報を表示するには、特権 EXEC モードで **debug ip eigrp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

no debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
ip-addr mask	（任意）デバッグ出力を、IP アドレスおよびネットワーク マスクにより定義される範囲内のメッセージに制限します。
neighbor *nbr-addr*	（任意）デバッグ出力を、指定したネイバーに制限します。
notifications	（任意）デバッグ出力を、EIGRP プロトコル イベントおよび通知に制限します。
summary	（任意）デバッグ出力を集約ルート処理に制限します。
user-interface	（任意）デバッグ出力をユーザ イベントに制限します。

デフォルト

キーワードまたは引数を指定しない場合、IPv4 ASDM のデバッグ メッセージのみ表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、インターフェイスで送受信されるパケットの分析に役立ちます。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug ip eigrp** コマンドの出力例を示します。

```
hostname# debug ip eigrp

IP-EIGRP Route Events debugging is on

EIGRP-IPv4(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.0.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.43.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.43.0 255.255.255.0 metric 371200 -
256000 115200
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.246.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.246.0 255.255.255.0 metric 46310656 -
45714176 596480
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.40.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.40.0 255.255.255.0 metric 2272256 -
1657856 614400
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.245.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.245.0 255.255.255.0 metric 40622080 -
40000000 622080
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.244.0 255.255.255.0, - do advertise out
Ethernet0/1
```

表 10-1 に、この出力で表示される重要なフィールドの説明を示します。

表 10-1　debug ip eigrp のフィールドの説明

フィールド	説明
IP-EIGRP:	IP EIGRP メッセージを示します。
Ext	後続のアドレスが内部ルートではなく外部ルートであることを示します。内部ルートには、Int というラベルが付加されます。
M	計算済みのメトリックを示します。計算済みのメトリックには、SM フィールドの値、および当該ルータとネイバーとの間のコストが含まれます。最初の数値は複合メトリックです。次の 2 つの数値はそれぞれ逆帯域幅および遅延です。
SM	ネイバーがレポートしたとおりのメトリックを表示します。

関連コマンド

コマンド	説明
debug eigrp packets	EIGRP パケットのデバッグ情報を表示します。

debug ipsec-over-tcp

IPSec-over-TCP のデバッグ情報を表示するには、特権 EXEC モードで **debug ipsec-over-tcp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、IPSec-over-TCP のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、IPSec-over-TCP のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug ipsec-over-tcp
debug ipsec-over-tcp  enabled at level 1
hostname# show debug
debug ipsec-over-tcp  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ipv6

ipv6 のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ipv6** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ipv6 {icmp | interface | mld | nd | packet | routing}

no debug ipv6 {icmp | interface | nd | packet | routing}

構文の説明

icmp	ICMPv6 ネイバー探索トランザクションを除く IPv6 ICMP トランザクションのデバッグ メッセージを表示します。
interface	IPv6 インターフェイスのデバッグ情報を表示します。
mld	Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）のデバッグ メッセージを表示します。
nd	ICMPv6 ネイバー探索トランザクションのデバッグ メッセージを表示します。
packet	IPv6 パケットのデバッグ メッセージを表示します。
routing	IPv6 ルーティング テーブル アップデートおよびルート キャッシュ アップデートのデバッグ メッセージを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug ipv6 icmp** コマンドの出力例を示します。

```
hostname# debug ipv6 icmp
```

```
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

関連コマンド

コマンド	説明
ipv6 icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP メッセージのアクセス ルールを定義します。
ipv6 address	1 つ以上の IPv6 アドレスを持つインターフェイスを設定します。
ipv6 nd dad attempts	重複アドレス検出時に実行するネイバー探索試行の回数を定義します。
ipv6 route	IPv6 ルーティング テーブル内にスタティック エントリを定義します。

debug iua-proxy

IUA プロキシのデバッグ情報を表示するには、特権 EXEC モードで **debug iua-proxy** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug iua-proxy [*level*]

no debug iua-proxy

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、IUA プロキシのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、IUA プロキシのデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug iua-proxy
debug iua-proxy  enabled at level 1
hostname# show debug
debug iua-proxy  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug kerberos

Kerberos 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug kerberos** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug kerberos [*level*]

no debug kerberos

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、Kerberos のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、Kerberos のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug kerberos
debug kerberos  enabled at level 1
hostname# show debug
debug kerberos  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug l2tp

L2TP のデバッグ情報を表示するには、特権 EXEC モードで **debug l2tp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug l2tp {**data** | **error** | **event** | **packet**} *level*

no debug l2tp {**data** | **error** | **event** | **packet**} *level*

構文の説明

data	データ パケットのトレース情報を表示します。
error	エラー イベントを表示します。
event	L2TP 接続イベントを表示します。
packet	パケット トレース情報を表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、接続イベントに関する L2TP デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、L2TP デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event enabled at level 1
```

```
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ldap

LDAP のデバッグ情報を表示するには、特権 EXEC モードで **debug ldap** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ldap [*level*]

no debug ldap

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、LDAP のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、LDAP のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug ldap
debug ldap  enabled at level 1
hostname# show debug
debug ldap  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mac-address-table

MAC アドレス テーブルのデバッグ メッセージを表示するには、特権 EXEC モードで **debug mac-address-table** コマンドを使用します。MAC アドレス テーブルのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug mac-address-table [*level*]

no debug mac-address-table [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、MAC アドレス テーブルのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug mac-address-table
```

関連コマンド

コマンド	説明
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

コマンド	説明
show debug	イネーブルなデバッガをすべて表示します。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

debug menu

特定機能の詳細なデバッグ情報を表示するには、特権 EXEC モードで **debug menu** コマンドを使用します。

debug menu

注意　**debug menu** コマンドは、Cisco TAC の指導の下でのみ使用する必要があります。

構文の説明

このコマンドは、Cisco TAC の指示の元でのみ使用する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

このコマンドは、Cisco TAC の指示の元でのみ使用する必要があります。

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mfib

MFIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mfib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*]

no debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*]

構文の説明

db	（任意）ルート データベースの動作に関するデバッグ情報を表示します。
group	（任意）マルチキャスト グループの IP アドレスです。
init	（任意）システム初期化アクティビティを表示します。
mrib	（任意）MFIB との通信のデバッグ情報を表示します。
pak	（任意）パケット転送動作のデバッグ情報を表示します。
ps	（任意）プロセス スイッチング動作のデバッグ情報を表示します。
signal	（任意）ルーティング プロトコルに対する MFIB シグナリングのデバッグ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MFIB データベース動作のデバッグ情報を表示する例を示します。

```
hostname# debug mfib db
MFIB IPv4 db debugging enabled
```

関連コマンド

コマンド	説明
show mfib	MFIB 転送エントリおよびインターフェイスを表示します。

debug mgcp

MGCP アプリケーション インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug mgcp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug mgcp {**messages** | **parser** | **sessions**}

no debug mgcp {**messages** | **parser** | **sessions**}

messages	MGCP メッセージに関するデバッグ情報を表示します。
parser	MGCP メッセージの解析に関するデバッグ情報を表示します。
sessions	MGCP セッションに関するデバッグ情報を表示します。

デフォルト

すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug mgcp コマンドは、mgcp インスペクションに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、MGCP アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug mgcp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect mgcp	MGCP アプリケーション インスペクションをイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
show mgcp	セキュリティ アプライアンスを通じて確立された MGCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。

debug mmp

MMP イベントのインスペクションを表示するには、特権 EXEC モードで **debug mmp** コマンドを使用します。MMP イベントのインスペクションの表示を停止するには、このコマンドの **no** 形式を使用します。

debug mmp

no debug mmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、MMP イベントのインスペクションを表示する **debug mmp** コマンドの使用例を示します。

```
hostname# debug mmp
ciscoasa5520-tfw-cuma/admin(config-pmap)# MMP:: received 28 bytes from outside:1
72.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: version OLWP-2.0
MMP status: 0
MMP:: forward 28/28 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: version OLWP-2.0
MMP:: session-id: 41A3D410-8B10-4DEB-B15C-B2B4B0D22055
MMP status: 201
MMP:: forward 85/85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 196
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 200/196
MMP:: forward 265/265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 198
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 202/198
MMP:: forward 267/267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 67
```

```
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 71/67
MMP:: forward 135/135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: content-length: 32
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 36/32
MMP:: forward 100/100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 151
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 155/151
MMP:: forward 220/220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
```

関連コマンド

コマンド	説明
inspect mmp	MMP インスペクション エンジンを設定します。
show debug mmp	MMP インスペクション モジュールの現在のデバッグ設定を表示します。
show mmp	既存の MMP セッションに関する情報を表示します。

debug module-boot

SSM ブート プロセスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug module-boot** コマンドを使用します。SSM ブート プロセスのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug module-boot [*level*]

no debug module-boot [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、SSM ブート プロセスのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug module-boot
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。

コマンド	説明
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug mrib

MRIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mrib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mrib {**client** | **io** | **route** [*group*] | **table**}

no debug mrib {**client** | **io** | **route** [*group*] | **table**}

構文の説明

client	MRIB クライアント管理アクティビティのデバッグをイネーブルにします。
io	MRIB I/O イベントのデバッグをイネーブルにします。
route	MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
group	指定したグループの MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
table	MRIB テーブル管理アクティビティのデバッグをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MRIB I/O イベントのデバッグをイネーブルにする方法の例を示します。

```
hostname# debug mrib io
IPv4 MRIB io debugging is on
```

関連コマンド

コマンド	説明
show mrib client	MRIB クライアント接続に関する情報を表示します。
show mrib route	MRIB テーブルのエントリを表示します。

debug nac

NAC フレームワーク イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug nac** コマンドを使用します。NAC デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nac {**all** | **auth** | **errors** | **events**}

no debug nac {**all** | **auth** | **errors** | **events**}

構文の説明

all	すべての NAC 情報に関するデバッグ メッセージのロギングをイネーブルにします。
auth	NAC 認証の要求および応答に関するデバッグ メッセージのロギングをイネーブルにします。
errors	NAC セッション エラーのロギングをイネーブルにします。
events	NAC セッション イベントのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、初期化、例外リスト一致、ACS トランザクション、クライアントレス認証、デフォルト ACL アプリケーション、および再検証の各タイプの NAC イベントをログに記録します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての NAC セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug nac events
hostname#
```

次に、すべての NAC デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug nac all
hostname#
```

次に、すべての NAC デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug nac
hostname#
```

関連コマンド

コマンド	説明
debug eap	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
show vpn-session_summary.db	IPSec、WebVPN、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

debug ntdomain

NT ドメイン認証のデバッグ情報を表示するには、特権 EXEC モードで **debug ntdomain** コマンドを使用します。NT ドメインのデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ntdomain [*level*]

no debug ntdomain

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、NT ドメインのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、NT ドメインのデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug ntdomain
debug ntdomain  enabled at level 1
hostname# show debug
debug ntdomain  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ntp

NTP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ntp** コマンドを使用します。NTP のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

no debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

構文の説明

adjust	NTP クロックの調整に関するメッセージを表示します。
authentication	NTP 認証に関するメッセージを表示します。
events	NTP イベントに関するメッセージを表示します。
loopfilter	NTP ループ フィルタに関するメッセージを表示します。
packets	NTP パケットに関するメッセージを表示します。
params	NTP クロック パラメータに関するメッセージを表示します。
select	NTP クロックの選択に関するメッセージを表示します。
sync	NTP クロックの同期に関するメッセージを表示します。
validity	NTP ピア クロックの有効性に関するメッセージを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、NTP のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ntp events
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
show debug	イネーブルなデバッガをすべて表示します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

debug ospf

OSPF ルーティング プロセスに関するデバッグ情報を表示するには、特権 EXEC モードで **debug ospf** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** [**external** | **inter** | **intra**] | **tree**]

no debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** [**external** | **inter** | **intra**] | **tree**]

構文の説明

adj	（任意）OSPF 隣接イベントのデバッグをイネーブルにします。
database-timer	（任意）OSPF タイマー イベントのデバッグをイネーブルにします。
events	（任意）OSPF イベントのデバッグをイネーブルにします。
external	（任意）SPF デバッグを外部イベントに制限します。
flood	（任意）OSPF フラッディングのデバッグをイネーブルにします。
inter	（任意）SPF デバッグをエリア間イベントに制限します。
intra	（任意）SPF デバッグをエリア内イベントに制限します。
lsa-generation	（任意）OSPF サマリー LSA 生成のデバッグをイネーブルにします。
packet	（任意）受信済みの OSPF パケットのデバッグをイネーブルにします。
retransmission	（任意）OSPF 再送信イベントのデバッグをイネーブルにします。
spf	（任意）OSPF の最短パス優先計算のデバッグをイネーブルにします。**external**、**inter**、および **intra** キーワードを使用することで、SPF デバッグ情報を制限できます。
tree	（任意）OSPF データベース イベントのデバッグをイネーブルにします。

デフォルト

キーワードを指定しないと、すべての OSPF デバッグ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug ospf events** コマンドの出力例を示します。

```
hostname# debug ospf events
ospf event debugging is on

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

関連コマンド

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

debug parser cache

CLI パーサーのデバッグ情報を表示するには、特権 EXEC モードで **debug parser cache** コマンドを使用します。CLI パーサーのデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug parser cache [*level*]

no debug parser cache

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、CLI パーサーのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。**show debug** コマンドの出力の前後に、CLI パーサーのデバッグ メッセージが表示されています。

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug phone-proxy

電話プロキシ インスタンスのデバッグ メッセージを表示するには、特権 EXEC モードで **debug phone-proxy** コマンドを使用します。電話プロキシ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

no debug phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

構文の説明

errors	（任意）電話プロキシ エラーのデバッグ メッセージを表示します。
events	（任意）電話プロキシ イベントのデバッグ メッセージを表示します。
media	（任意）SIP インスペクションおよび Skinny インスペクションのメディア セッションのデバッグ メッセージを表示します。
signaling	（任意）SIP インスペクションおよび Skinny インスペクションのシグナリング セッションのデバッグ メッセージを表示します。
tftp	（任意）CTL ファイルの作成、コンフィギュレーション ファイルの解析など、TFTP インスペクションのデバッグ メッセージを表示します。

デフォルト

debug phone-proxy コマンドでオプションを指定しない場合、すべての電話プロキシ デバッグ メッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

debug phone-proxy コマンドは、電話プロキシ アクティビティに関する詳細情報を表示します。**no debug phone-proxy** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、**debug phone-proxy** コマンドを使用して、電話プロキシのコンフィギュレーション ファイル要求に関する成功 TFTP トランザクションを表示する例を示します。

```
hostname(config)# debug phone-proxy tftp
PP: 98.208.49.30/1028 requesting SEP00070E364804.cnf.xml.sgn
PP: opened 0x33952aa2
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
        Received Block 1
PP: Acked Block #1 from 98.208.49.30/1028 to 192.168.200.101/39514
```

```
          .... [snip].....
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
       Received Block 10
PP: Acked Block #10 from 98.208.49.30/1028 to 192.168.200.101/39514
PP: Installed application redirect rule from 98.208.49.30 to 192.168.200.101 using
redirect port 2000 and secure port 2443
PP: Modifying to TLS as the transport layer protocol.
PP: Modifying to encrypted mode.
PP: Data Block 1 forwarded from 192.168.200.101/39514 to 98.208.49.30/1028
PP: Received ACK Block 1 from outside:98.208.49.30/1028 to inside:192.168.200.101
          ..... [snip] ....
PP: Data Block 11 forwarded to 98.208.49.30/1028
PP: Received ACK Block 11 from outside:98.208.49.30/1028 to inside:192.168.200.101
PP: TFTP session complete, all data sent
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show running-config phone-proxy	Phone Proxy 固有の情報を表示します。

debug pim

PI M のデバッグ情報を表示するには、特権 EXEC モードで **debug pim** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

no debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

構文の説明

df-election	（任意）PIM 双方向 DF 選出メッセージ処理のデバッグ メッセージを表示します。
group *group*	（任意）指定したグループのデバッグ情報を表示します。*group* には、値として次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
interface *if_name*	（任意）**df-election** キーワードを指定してこのコマンドを使用すると、DF 選出のデバッグ表示が、指定したインターフェイスの情報に制限されます。 **df-election** キーワードを指定せずにこのコマンドを使用すると、指定したインターフェイスの PIM エラー メッセージが表示されます。 **（注）** **debug pim interface** コマンドでは、PIM プロトコル アクティビティ メッセージは表示されず、エラー メッセージのみ表示されます。PIM プロトコル アクティビティのデバッグ情報を表示するには、**interface** キーワードを指定せずに **debug pim** コマンドを使用します。**group** キーワードを使用することで、指定したマルチキャスト グループに表示を制限できます。
neighbor	（任意）送受信された PIM hello メッセージのみ表示します。
rp *rp*	（任意）次のいずれかを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　送受信された PIM パケットおよび PIM 関連のイベントをログに記録します。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例　次に、**debug pim** コマンドの出力例を示します。

```
hostname# debug pim
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.6
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16
PIM: Send Prune on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.24.84.16/28
PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Ethernet1)
```

関連コマンド

コマンド	説明
show pim group-map	グループ対プロトコルのマッピング テーブルを表示します。
show pim interface	PIM のインターフェイス固有情報を表示します。
show pim neighbor	PIM ネイバー テーブル内のエントリを表示します。

debug pix acl

PIX ACL のデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix acl** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix acl

no debug pix acl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り debug コマンドを使用してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix acl
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix cls

PIX CLS のデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix cls** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix cls

no debug pix cls

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り debug コマンドを使用してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix cls
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix pkt2pc

uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされるイベントをトレースするデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix pkt2pc** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix pkt2pc

no debug pix pkt2pc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされるイベントをトレースするデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix pkt2pc
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix process

xlate および 2 番めの接続処理のデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix process** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix process

no debug pix process

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、xlate および 2 番めの接続処理のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix process
```

関連コマンド

コマンド	説明
debug pix pkt2pc	uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされるイベントをトレースするデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix uauth

pix uauth のデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix uauth** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix uauth

no debug pix uauth

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り debug コマンドを使用してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix uauth
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pptp

PPTP のデバッグ メッセージを表示するには、特権 EXEC モードで **debug pptp** コマンドを使用します。PPTP のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pptp [*level*]

no debug pptp [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug pptp** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、PPTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pptp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect pptp	PPTP アプリケーション インスペクションをイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug radius

AAA のデバッグ メッセージを表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。RADIUS メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug radius [**all** | **decode** | **session** | **user** *username*]]

no debug radius

構文の説明

all	（任意）すべてのユーザおよびセッションに関する RADIUS デバッグ メッセージ（デコードされた RADIUS メッセージを含む）を表示します。
decode	（任意）RADIUS メッセージのデコードされた内容を表示します。16 進数形式の値、およびこれらの値の、人が判読できるデコード済みバージョンを含む、すべての RADIUS パケットの内容が表示されます。
session	（任意）セッション関連の RADIUS メッセージを表示します。送受信された RADIUS メッセージのパケット タイプは表示されますが、パケットの内容は表示されません。
user	（任意）特定ユーザの RADIUS デバッグ メッセージを表示します。
username	表示するメッセージの所有者であるユーザを指定します。**user** キーワードを指定した場合に限り有効です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug radius コマンドは、セキュリティ アプライアンスと RADIUS AAA サーバとの間の RADIUS メッセージングに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、デコードされた RADIUS メッセージの例を示します。この RADIUS メッセージはアカウンティング パケットです。

```
hostname(config)# debug radius decode
hostname(config)# RADIUS packet decode (accounting request)
```

```
--------------------------------------
Raw packet data (length = 216).....
i
Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30 78 31 33 30 31 32 39 66 65                       |  0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72                                |  browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e    |  ip:source-ip=10.
31 2e 31 2e 31 30                                   |  1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 70 6f 72 74 3d 33    |  ip:source-port=3
34 31 33                                            |  413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69    |  ip:destination-i
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35    |  p=10.2.0.50
```

```
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70    |  ip:destination-p
6f 72 74 3d 38 30                                  |  ort=80
```

関連コマンド

コマンド	説明
show running-config	セキュリティ アプライアンス上で実行されているコンフィギュレーションを表示します。

debug redundant-interface

冗長インターフェイスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug redundant-interface** コマンドを使用します。冗長インターフェイスのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug redundant-interface [*level*]

no debug redundant-interfac [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、冗長インターフェイスのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug redundant-interface
```

関連コマンド

コマンド	説明
interface redundant	冗長インターフェイスを作成します。
member-interface	物理インターフェイスを冗長インターフェイスに割り当てます。
redundant-interface	冗長インターフェイス ペア内のアクティブ インターフェイスを変更します。
show debug	イネーブルなデバッガをすべて表示します。

debug rip

RIP のデバッグ情報を表示するには、特権 EXEC モードで **debug rip** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug rip [**database** | **events**]

no debug rip [**database** | **events**]

構文の説明

database	RIP データベース イベントを表示します。
events	RIP 処理イベントを表示します。

デフォルト

すべての RIP イベントがデバッグ出力に表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	**database** キーワードと **events** キーワードが追加されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug rip** コマンドの出力例を示します。

```
hostname# debug rip

RIP: broadcasting general request on GigabitEthernet0/1
RIP: broadcasting general request on GigabitEthernet0/2
RIP: Received update from 10.89.80.28 on GigabitEthernet0/1
    10.89.95.0 in 1 hops
    10.89.81.0 in 1 hops
    10.89.66.0 in 2 hops
    172.31.0.0 in 16 hops (inaccessible)
    0.0.0.0 in 7 hops
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/1 (10.89.64.31)
```

```
    subnet 10.89.94.0, metric 1
    172.31.0.0 in 16 hops (inaccessible)
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/2 (10.89.94.31)
    subnet 10.89.64.0, metric 1
    subnet 10.89.66.0, metric 3
    172.31.0.0 in 16 hops (inaccessible)
    default 0.0.0.0, metric 8
RIP: bad version 128 from 192.168.80.43
```

関連コマンド

コマンド	説明
router rip	RIP プロセスを設定します。
show running-config rip	実行コンフィギュレーションの RIP コマンドを表示します。

debug rtp

H.323 および SIP インスペクションに関連する RTP パケットのデバッグ情報およびエラー メッセージを表示するには、特権 EXEC モードで **debug rtp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug rtp [*level*]

no debug rtp [*level*]

構文の説明

level	（任意）デバッグのオプション レベルを指定します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug rtp** コマンドを使用して RTP パケットのデバッグをイネーブルにする例を示します。

```
hostname# debug rtp 255
debug rtp  enabled at level 255
```

関連コマンド

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。

コマンド	説明
rtp-conformance	H.323 および SIP のプロトコル適合のために、ピンホールをフローする RTP パケットをチェックします。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

debug rtsp

RTSP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug rtsp** コマンドを使用します。RTSP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug rtsp [*level*]

no debug rtsp [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug rtsp** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、RTSP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug rtsp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect rtsp	RTSP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug sdi

SDI 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug sdi** コマンドを使用します。SDI デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sdi [*level*]

no debug sdi

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、SDI デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、SDI デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug sdi
debug sdi  enabled at level 1
hostname# show debug
debug sdi  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug sequence

すべてのデバッグ メッセージの先頭にシーケンス番号を追加するには、特権 EXEC モードで **debug sequence** コマンドを使用します。デバッグ シーケンス番号の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sequence [*level*]

no debug sequence

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- デバッグ メッセージのシーケンス番号はディセーブルです。
- *level* のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージのシーケンス番号をイネーブルにする例を示します。**debug parser cache** コマンドは、CLI パーサーのデバッグ メッセージをイネーブルにします。**show debug** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。表示されている CLI パーサーのデバッグ メッセージでは、各メッセージの前にシーケンス番号が追加されています。

```
hostname# debug sequence
debug sequence  enabled at level 1
```

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence  enabled at level 1
1: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug session-command

SSM とのセッションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug session-command** コマンドを使用します。セッションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug session-command [*level*]

no debug session-command [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、セッションのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug session-command
```

関連コマンド

コマンド	説明
session	SSM とのセッション。

debug sip

SIP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sip** コマンドを使用します。SIP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sip [**ha**]

no debug sip [**ha**]

構文の説明

ha	（任意）SIP ステートフル フェールオーバー メッセージを表示します。 アクティブ ユニットに対する **debug sip** コマンドでこのキーワードを使用すると、SIP 状態情報がスタンバイ ユニットに送信されるときにデバッグ メッセージが表示されます。スタンバイ ユニットに対する **debug sip** コマンドでこのキーワードを使用すると、アクティブ ユニットから状態更新が受信されるときにデバッグ メッセージが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	**ha** キーワードが追加されました。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、アクティブ ユニットまたはフェールオーバー ペア内のフェールオーバー グループに対して実行した **debug sip** コマンドの出力例を示します。

```
hostname# debug sip ha
SIP HA:    Sending    update SESSION message from faddr 10.132.80.120/5060 laddr
10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:
State:1

SIP HA:    msg sent to peer successful  Version: 1 Action: update Object: session

SIP HA:    Sending    update TX message from faddr 10.132.80.120/5060laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

次に、スタンバイ ユニットまたはフェールオーバー ペア内のフェールオーバー グループに対して実行した **debug sip** コマンドの出力例を示します。

```
hostname# debug sip ha
SIP HA:    Message    received from peer, Version: 1 Action: add Object: session

SIP HA:    Created    SIP session for faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120: 1
total

SIP HA:    Message    received from peer, Version: 1 Action: add Object: tx

SIP HA:    Found an existing session faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:

SIP HA:    Created    SIP Transaction    for faddr 10.132.80.120/5060 to   laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect sip	SIP アプリケーション インスペクションをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
show sip	セキュリティ アプライアンスを通じて確立された SIP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug skinny

SCCP（Skinny）アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug skinny** コマンドを使用します。SCCP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug skinny [*level*]

no debug skinny [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug skinny** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、SCCP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug skinny
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect skinny	SCCP アプリケーション インスペクションをイネーブルにします。
show skinny	セキュリティ アプライアンスを通じて確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug sla monitor

SLA モニタ動作のデバッグ メッセージを表示するには、特権 EXEC モードで **debug sla monitor** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sla monitor [**error** | **trace**] [*sla-id*]

no debug sla monitor [*sla-id*]

構文の説明

error	（任意）IP SLA モニタのエラー メッセージを出力します。
sla-id	（任意）デバッグする SLA の ID。
trace	（任意）IP SLA モニタのトレース メッセージを出力します。

デフォルト

デフォルトでは、エラー メッセージとトレース メッセージの両方が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

同時にデバッグできる SLA 動作は 32 個のみです。

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、SLA 動作のエラー デバッグをイネーブルにする例を示します。

```
hostname(config)# debug sla monitor error
```

次に、指定した SLA 動作に関する SLA 動作トレース メッセージを表示する例を示します。

```
hostname(config)# debug sla monitor trace 123
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

debug sqlnet

SQL*Net アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sqlnet** コマンドを使用します。SQL*Net アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sqlnet [*level*]

no debug sqlnet [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug sqlnet** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、SQL*Net アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug sqlnet
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect sqlnet	SQL*Net アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SQL*Net など、さまざまな接続タイプの接続状態を表示します。

debug ssh

SSH に関連するデバッグ情報およびエラー メッセージを表示するには、特権 EXEC モードで **debug ssh** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ssh [*level*]

no debug ssh [*level*]

構文の説明

level	（任意）デバッグのオプション レベルを指定します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug ssh 255** コマンドの出力例を示します。

```
hostname# debug ssh 255
debug ssh  enabled at level 255
SSH2 0: send: len 64 (includes padlen 17)
SSH2 0: done calc MAC out #239
SSH2 0: send: len 32 (includes padlen 7)
SSH2 0: done calc MAC out #240
SSH2 0: send: len 64 (includes padlen 15)
SSH2 0: done calc MAC out #241
SSH2 0: send: len 32 (includes padlen 16)
SSH2 0: done calc MAC out #242
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #243
```

```
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #244
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #245
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #246
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #247
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #248
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #249
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #250
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #251
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #252
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #253
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #254
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #255
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #256
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #257
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #258
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンスとのアクティブ SSH セッションに関する情報を表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

debug sunrpc

RPC アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sunrpc** コマンドを使用します。RPC アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sunrpc [*level*]

no debug sunrpc [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug sunrpc** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、RPC アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug sunrpc
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
show conn	RPC を含む各種接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug switch ilpm

組み込みスイッチ（ASA 5505 適応型セキュリティ アプライアンスなど）を使用するモデル、または PoE に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug switch ilpm** コマンドを使用します。PoE のデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug switch ilpm [**events** | **errors**] [*level*]

no debug switch ilpm [**events** | **errors**] [*level*]

構文の説明

errors	（任意）エラーがある場合にトラブルシューティング情報を表示します。
events	（任意）PoE イベントを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトでは、キーワードを指定しない場合、イベントとエラーの両方が表示されます。デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、PoE ポートのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug switch ilpm
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。

コマンド	説明
debug switch manager	VLAN 割り当ておよび **switchport** コマンドが原因のイベントおよびエラーに関するデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug switch manager

組み込みスイッチ（ASA 5505 適応型セキュリティ アプライアンスなど）を使用するスイッチ ポート モデル、VLAN 割り当て、および **switchport** コマンドが原因のイベントおよびエラーに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug switch manager** コマンドを使用します。スイッチ ポートに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug switch manager [**events** | **errors**] [*level*]

no debug switch manager [**events** | **errors**] [*level*]

構文の説明

errors	（任意）エラーがある場合にトラブルシューティング情報を表示します。
events	（任意）スイッチ マネージャ イベントを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトでは、キーワードを指定しない場合、イベントとエラーの両方が表示されます。デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、スイッチ ポートのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug switch manager
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。

コマンド	説明
debug switch ilpm	PoE のデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug tacacs

TACACS+ のデバッグ メッセージを表示するには、特権 EXEC モードで **debug tacacs** コマンドを使用します。TACACS+ のデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug tacacs [**session** | **user** *username*]

no debug tacacs [**session** | **user** *username*]

構文の説明

session	セッション関連の TACACS+ のデバッグ メッセージを表示します。
user	ユーザ固有の TACACS+ のデバッグ メッセージを表示します。一度に 1 人のユーザのみの TACACS+ デバッグ メッセージを表示できます。
username	表示する TACACS+ デバッグ メッセージの所有者であるユーザを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、TACACS+ デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、TACACS+ デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug tacacs user admin342
hostname# show debug
debug tacacs user admin342
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug tcp-map

TCP アプリケーション インスペクション マップのデバッグ メッセージを表示するには、特権 EXEC モードで **debug tcp-map** コマンドを使用します。TCP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug tcp-map

no debug tcp-map

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、TCP アプリケーション インスペクション マップのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、TCP アプリケーション インスペクション マップのデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug timestamps

すべてのデバッグ メッセージの先頭にタイムスタンプ情報を追加するには、特権 EXEC モードで **debug timestamps** コマンドを使用します。デバッグ タイムスタンプの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug timestamps [*level*]

no debug timestamps

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- デバッグ タイムスタンプ情報はディセーブルです。
- *level* のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージのタイムスタンプをイネーブルにする例を示します。**debug parser cache** コマンドは、CLI パーサーのデバッグ メッセージをイネーブルにします。**show debug** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。表示されている CLI パーサーのデバッグ メッセージでは、各メッセージの前にタイムスタンプが追加されています。

```
hostname# debug timestamps
debug timestamps  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
```

```
hostname# show debug
1982769.770000000: parser cache: try to match 'show debug' in exec mode
1982769.770000000: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug vpn-sessiondb

VPN セッション データベースのデバッグ情報を表示するには、特権 EXEC モードで **debug vpn-sessiondb** コマンドを使用します。VPN セッション データベースのデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug vpn-sessiondb [*level*]

no debug vpn-sessiondb

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、VPN セッション データベースのこデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、VPN セッション データベースのデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug vpn-sessiondb
debug vpn-sessiondb  enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug wccp

WCCP イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug wccp** コマンドを使用します。WCCP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug wccp {**events | packets | subblocks**}

no debug wccp {**events | packets | subblocks**}

構文の説明

events	WCCP セッション イベントのロギングをイネーブルにします。
packets	WCCP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
subblocks	WCCP サブブロックに関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての WCCP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug wccp events
hostname#
```

次に、WCCP パケットのデバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug wccp packets
hostname#
```

次に、WCCP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug wccp
hostname#
```

関連コマンド

コマンド	説明
wccp	WCCP のサポートをイネーブルにします。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug webvpn

WebVPN のデバッグ メッセージをログに記録するには、特権 EXEC モードで **debug webvpn** コマンドを使用します。WebVPN のデバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

no debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

構文の説明

chunk	WebVPN 接続をサポートするために使用されるメモリ ブロックに関するデバッグ メッセージを表示します。
cifs	CIFS サーバと WebVPN ユーザの間の接続に関するデバッグ メッセージを表示します。
citrix	WebVPN を介した Citrix Metaframe サーバと Citrix ICA クライアントの間の接続に関するデバッグ メッセージを表示します。
failover	WebVPN 接続に影響する装置フェールオーバーに関するデバッグ メッセージを表示します。
html	WebVPN 接続を介して送信される HTML ページに関するデバッグ メッセージを表示します。
javascript	WebVPN 接続で送信された JavaScript に関するデバッグ メッセージを表示します。
request	WebVPN 接続を介して発行された要求に関するデバッグ メッセージを表示します。
response	WebVPN 接続を介して発行された応答に関するデバッグ メッセージを表示します。
svc	WebVPN を介した SSL VPN クライアントへの接続に関するデバッグ メッセージを表示します。
transformation	WebVPN コンテンツ変換に関するデバッグ メッセージを表示します。
url	WebVPN 接続を介して発行された Web サイト要求に関するデバッグ メッセージを表示します。
util	WebVPN リモート ユーザへの接続のサポートのために占有される CPU 使用率に関するデバッグ メッセージを表示します。
xml	WebVPN 接続で送信された JavaScript に関するデバッグ メッセージを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、CIFS に関する WebVPN デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、CIFS のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug webvpn cifs
INFO: debug webvpn cifs enabled at level 1.
hostname# show debug
debug webvpn cifs enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug xdmcp

XDMCP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug xdmcp** コマンドを使用します。XDMCP アプリケーション インスペクションのデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug xdmcp [*level*]

no debug xdmcp [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注） **debug xdmcp** コマンドをイネーブルにすると、通信量の多いネットワークでトラフィックが遅くなる可能性があります。

例

次に、XDMCP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug xdmcp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect xdmcp	XDMCP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug xml

XML パーサーのデバッグ情報を表示するには、特権 EXEC モードで **debug xml** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug xml [**element** | **event**]

no debug xml [**element** | **event**]

構文の説明

element	（任意）個々の XML 要素の処理に関連するデバッグ イベントを表示します。
event	（任意）XML 解析またはエラー イベントを表示します。

デフォルト

キーワードを指定しないと、すべての XML パーサー デバッグ メッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug xml element** コマンドの出力例を示します。

```
hostname# debug xml element
debug xml element enabled at level 1

XML Executes cmd: hostname hostname
XML Executes cmd: domain-name example.com
XML Executes cmd: names
XML Executes cmd: dns-guard
XML Executes cmd: !
XML Executes cmd: interface Ethernet0
XML Executes cmd:  nameif outside
```

```
XML Executes cmd:  security-level 0
XML Executes cmd:  ip address 192.168.5.151 255.255.255.0 standby 192.168.5.152
XML Executes cmd: interface Ethernet1
XML Executes cmd:  nameif inside
XML Executes cmd:  security-level 100
XML Executes cmd:  ip address 192.168.0.151 255.255.255.0 standby 192.168.0.152
XML Executes cmd: !
XML Executes cmd: boot system flash:/f
XML Executes cmd: ftp mode passive
XML Executes cmd: clock timezone jst 9
XML Executes cmd: dns server-group DefaultDNS
XML Executes cmd:  domain-name cisco.com
_tcp_listen: could not query index for interface 65535 port 23
XML Executes cmd: pager lines 24
XML Executes cmd: logging console debugging
XML Executes cmd: logging buffered debugging
XML Executes cmd: mtu outside 1500
XML Executes cmd: mtu inside 1500
XML Executes cmd: failover
XML Executes cmd: no asdm history enable
XML Executes cmd: arp timeout 14000
XML Executes cmd: route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
XML Executes cmd: timeout xlate 3:00:00
XML Executes cmd: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
XML Executes cmd: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
XML Executes cmd: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
XML Executes cmd: timeout uauth 0:05:00 absolute
XML Executes cmd: username user1 password mbO2jYs13AXlIAGa encrypted
XML Executes cmd: username sugi password EB3OP7Hu2hSu6x/7 encrypted
XML Executes cmd: http server enable
XML Executes cmd: http 0.0.0.0 0.0.0.0 outside
XML Executes cmd: no snmp-server location
XML Executes cmd: no snmp-server contact
XML Executes cmd: snmp-server enable traps snmp authentication linkup linkdown coldstart
XML Executes cmd: telnet timeout 5
XML Executes cmd: ssh timeout 5
XML Executes cmd: console timeout 0
XML Executes cmd: !
XML Executes cmd: class-map inspection_default
XML Executes cmd:  match default-inspection-traffic
XML Executes cmd: !
XML Executes cmd: !
XML Executes cmd: policy-map type inspect dns migrated_dns_map_1
XML Executes cmd:  parameters
XML Executes cmd:   message-length maximum 512
XML Executes cmd: policy-map global_policy
XML Executes cmd:  class inspection_default
XML Executes cmd:   inspect ftp
XML Executes cmd:   inspect h323 h225
XML Executes cmd:   inspect h323 ras
XML Executes cmd:   inspect netbios
XML Executes cmd:   inspect rsh
XML Executes cmd:   inspect rtsp
XML Executes cmd:   inspect skinny
XML Executes cmd:   inspect esmtp
XML Executes cmd:   inspect sqlnet
XML Executes cmd:   inspect sunrpc
XML Executes cmd:   inspect tftp
XML Executes cmd:   inspect sip
XML Executes cmd:   inspect xdmcp
XML Executes cmd: !
XML Executes cmd: service-policy global_policy global
```

```
XML error info: cmd-id 87 type info
XML Executes cmd: prompt hostname context
XML Executes cmd: crashinfo save disable
```

次に、**debug xml event** コマンドの出力例を示します。

```
hostname# debug xml event
debug xml event enabled at level 1

XML parsing: data = <con... len = 3176
Exit XML parser, ret code = 0
```

関連コマンド

コマンド	説明
show debug	各種の **debug** コマンドのデバッグ ステータスを表示します。

CHAPTER 11

default（crl configure）コマンド～ dynamic-access-policy-record コマンド

default（crl 設定）

すべての CRL パラメータをシステム デフォルト値に戻すには、crl 設定コンフィギュレーション モードで **default** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバで必要な場合のみ使用されます。

default

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•		•		

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、ca-crl コンフィギュレーション モードを開始して、CRL コマンド値をデフォルトに戻す例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（インターフェイス）

インターフェイス コマンドをシステム デフォルト値に戻すには、インターフェイス コンフィギュレーション モードで **default** コマンドを使用します。

default *command*

構文の説明

command	デフォルトに設定するコマンドを指定します。次に例を示します。 `default activation key`

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは実行時コマンドです。入力しても、アクティブなコンフィギュレーションの一部になりません。

例

次に、インターフェイス コンフィギュレーション モードを開始して、セキュリティ レベルをデフォルトに戻す例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# default security-level
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

default（時間範囲）

absolute コマンドおよび **periodic** コマンドの設定をデフォルトに戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

構文の説明

absolute	時間範囲が有効になる絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている有効時間範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。 この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。
to	「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

time-range コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute start** 時刻を経過した後にのみ評価の対象になり、**absolute end** 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、セキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

例

次に、**absolute** キーワードの動作をデフォルトに戻す例を示します。

```
hostname(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default-acl

ポスチャ検証が失敗した NAC フレームワーク セッションのデフォルトの ACL として使用されるように ACL を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **default-acl** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

[no] **default-acl** *acl-name*

構文の説明

acl-name	セッションに適用されるアクセス コントロール リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。セキュリティ アプライアンスは、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、セキュリティ アプライアンスはデフォルト ACL をリモート ホストのアクセス コントロール サーバから取得した ACL に置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。

また、セキュリティ アプライアンスは、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

例

次に、ポスチャ検証が成功する前に適用される ACL として acl-1 を指定する例を示します。

```
hostname(config-group-policy)# default-acl acl-1
hostname(config-group-policy)
```

次に、デフォルト グループ ポリシーから ACL を継承する例を示します。

```
hostname(config-group-policy)# no default-acl
```

```
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

default enrollment

すべての登録パラメータをシステム デフォルト値に戻すには、クリプト CA トラストポイント コンフィギュレーション モードで **default enrollment** コマンドを使用します。

default enrollment

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻す例を示します。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># default enrollment
hostname<ca-trustpoint>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	CRL コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

default-domain

グループ ポリシーのユーザのデフォルト ドメイン名を設定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

構文の説明

none	デフォルト ドメイン名がないことを指定します。デフォルト ドメイン名にヌル値を設定して、デフォルト ドメイン名を拒否します。デフォルトまたは指定したグループ ポリシーのデフォルト ドメイン名は継承されません。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

セキュリティ アプライアンスは、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPSec クライアントに渡します。このドメイン名は、トンネル パケットにのみ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

デフォルト ドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

例

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

default-group-policy

ユーザがデフォルトで継承する属性のセットを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **default-group-policy** コマンドを使用します。デフォルトのグループ ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *group-name*

no default-group-policy *group-name*

構文の説明

group-name	デフォルト グループの名前を指定します。

デフォルト

デフォルト グループ名は DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

バージョン	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn コンフィギュレーション モードの **default-group-policy** コマンドは廃止されました。このコマンドは、トンネル グループ一般属性モードの **default-group-policy** コマンドに置き換えられています。

使用上のガイドライン

バージョン 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

デフォルト グループ ポリシー DfltGrpPolicy には、セキュリティ アプライアンスが初期設定されています。この属性は、すべてのトンネル グループ タイプに適用できます。

例

次に、設定一般コンフィギュレーション モードを開始して、「standard-policy」という名前の IPSec LAN-to-LAN トンネル グループで、ユーザがデフォルトで継承する属性のセットを指定する例を示します。このコマンド セットでは、アカウンティング サーバ、認証サーバ、認可サーバ、およびアドレス プールを定義します。

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)# authorization-server-group aaa-server78
```

```
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-policy	グループ ポリシーを作成または編集します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

default-group-policy（webvpn）

WebVPN または電子メール プロキシ設定でグループ ポリシーが指定されない場合に使用するグループ ポリシーの名前を指定するには、さまざまなコンフィギュレーション モードで **default-group-policy** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

default-group-policy *groupname*

no default-group-policy

構文の説明

groupname	デフォルト グループ ポリシーとして使用する、設定済みのグループ ポリシーを指定します。**group-policy** コマンドを使用して、グループ ポリシーを設定します。

デフォルト

DfltGrpPolicy という名前のデフォルト グループ ポリシーは、常に、セキュリティ アプライアンスに存在します。この **default-group-policy** コマンドを使用すると、作成したグループ ポリシーを、WebVPN および電子メール プロキシ セッション用のデフォルト グループ ポリシーとして置き換えることができます。または、DfltGrpPolicy を編集することもできます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—

コマンド履歴

バージョン	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

WebVPN セッション、IMAP4S セッション、POP3S セッション、および SMTPS セッションには、指定されたグループ ポリシーまたはデフォルト グループ ポリシーが必要です。WebVPN の場合は、webvpn モードでこのコマンドを使用します。電子メール プロキシの場合、このコマンドは、該当する電子メール プロキシ モードで使用します。

バージョン 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

システムの DefaultGroupPolicy は編集できますが、削除はしないでください。DefaultGroupPolicy の AVP は、次のとおりです。

属性	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn 属性：	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	none

例

次に、WebVPN7 という名前の WebVPN のデフォルト グループ ポリシーを指定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

WebVPN ユーザのデフォルト アイドル タイムアウト値を設定するには、webvpn コンフィギュレーション モードで **default-idle-timeout** コマンドを使用します。デフォルトのタイムアウト値をコンフィギュレーションから削除し、デフォルトをリセットするには、このコマンドの **no** 形式を使用します。

デフォルト アイドル タイムアウトにより、セッションの失効を回避できます。

default-idle-timeout *seconds*

no default-idle-timeout

構文の説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒で、最大値は 1 日（86400 秒）です。

デフォルト

1800 秒（30 分）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ユーザのアイドル タイムアウトが定義されていない場合、値が 0 の場合、または値が有効な値の範囲外である場合に、セキュリティ アプライアンスでは、ここで設定した値が使用されます。

このコマンドには、短い時間を設定することを推奨します。これは、クッキーをディセーブルにするブラウザ設定（またはプロンプトでクッキーを要求してから拒否するブラウザ設定）によって、ユーザが接続していないにもかかわらずセッション データベースに表示されることがあるためです。許可される最大接続数が 1 に設定されている（**vpn-simultaneous-logins** コマンド）場合、最大接続数がすでに存在することがデータベースによって示されるため、ユーザは再ログインすることができません。アイドル タイムアウトを短く設定すると、このようなファントム セッションを迅速に削除し、ユーザが再ログインできるようにすることができます。

例

次に、デフォルト アイドル タイムアウトを 1200 秒（20 分）に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許可される同時 VPN セッションの最大数を設定します。グループ ポリシー モードまたはユーザ名モードを使用します。

default-information（EIGRP）

EIGRP ルーティング プロセスのデフォルト ルート情報候補を制御するには、ルータ コンフィギュレーション モードで **default-information** コマンドを使用します。着信更新または発信更新で EIGRP デフォルト ルート情報候補を非表示にするには、このコマンドの **no** 形式を使用します。

default-information {**in** | **out**} [*acl-name*]

no default-information {**in** | **out**}

構文の説明

acl-name	（任意）名前付き標準アクセス リスト。
in	外部のデフォルト ルーティング情報を受け入れるように EIGRP を設定します。
out	外部ルーティング情報をアドバタイズするように EIGRP を設定します。

デフォルト

外部ルートが受け入れられ、送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

アクセス リストが指定されたこのコマンドまたは **default-information** コマンドの **no** 形式のみが実行コンフィギュレーションに表示されます。これは、デフォルト ルーティング情報候補がデフォルトで受け入れられ、送信されるためです。このコマンドの **no** 形式には、*acl-name* 引数はありません。

例

次に、外部デフォルト ルート情報またはデフォルト ルート情報候補の受領をディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no default-information in
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

default-information originate（OSPF）

OSPF ルーティング ドメインへのデフォルト外部ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]]

構文の説明

always	（任意）ソフトウェアにデフォルト ルートがあるかどうかにかかわらず、常に、デフォルト ルートをアドバタイズします。
metric *value*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type {1 | 2}	（任意）OSPF ルーティング ドメインにアドバタイズするデフォルト ルートに関連付けられている外部リンク タイプ 有効な値は、次のとおりです。 • **1**：タイプ 1 の外部ルート • **2**：タイプ 2 の外部ルート
route-map *name*	（任意）適用するルート マップ名。

デフォルト

デフォルト値は次のとおりです。

- **metric** *value* は 1 です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの **no** 形式をオプションのキーワードおよび引数とともに使用すると、コマンドからオプションの情報のみが削除されます。たとえば、**no default-information originate metric** *3* と入力すると、実行コンフィギュレーションのコマンドから **metric** *3* オプションが削除されます。コマンド全体を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式をオプションなしで使用します（**no default-information originate**）。

例

次に、オプションのメトリックおよびメトリック タイプとともに **default-information originate** コマンドを使用する例を示します。

```
hostname(config-router)# default-information originate always metric 3 metric-type 2
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

default-information originate（RIP）

RIP へのデフォルト ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]

構文の説明

route-map *name*	（任意）適用するルート マップ名。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

default-information originate コマンドで参照されるルート マップは拡張アクセス リストを使用できません。標準のアクセス リストを使用します。

例

次に、デフォルト ルートを RIP に生成する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# default-information originate
```

関連コマンド

コマンド	説明
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

default-language

クライアントレス SSL VPN ページに表示されるデフォルト言語を設定するには、webvpn コンフィギュレーション モードで **default-language** コマンドを使用します。

default-language *language*

構文の説明

language	事前にインポート済みの変換テーブル名を指定します。

デフォルト

デフォルト言語は en-us（米国で使用されている英語）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

デフォルト言語は、クライアントレス SSL VPN ユーザがログイン前に、最初にセキュリティ アプライアンスに接続するときに表示されます。その後、トンネル グループ設定またはトンネル ポリシー設定およびこれらの設定が参照するカスタマイズに基づいて言語が表示されます。

例

次に、*Sales* という名前を指定して、デフォルト言語を中国語に変更する例を示します。

```
hostname(config-webvpn)# default-language zh
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

default-metric

再配布されるルートの EIGRP メトリックを指定するには、ルータ コンフィギュレーション モードで **default-metric** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

構文の説明

bandwidth	ルートの最小帯域幅（KB/秒単位）。有効な値は、1 ～ 4294967295 です。
delay	ルート遅延（10 マイクロ秒単位）。有効な値は、1 ～ 4294967295 です。
reliability	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
loading	ルートの有効な帯域幅。1 ～ 255 の数値で表されます（255 は 100 % のロード）。
mtu	許可する MTU の最小値（バイト単位）。有効な値は 1 ～ 65535 です。

デフォルト

デフォルト メトリックなしで再配布できるのは、接続されているルートのみです。再配布される接続ルートのメトリックは、0 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

redistribute コマンドで **metric** キーワードおよび属性を使用しない場合は、デフォルト メトリックを使用して、EIGRP にプロトコルを再配布する必要があります。メトリックのデフォルトは、さまざまなネットワークで機能するよう慎重に設定されています。値を変更する場合は、最大限の注意を払うようにしてください。スタティック ルートから再配布する場合のみ、同じメトリックを維持できます。

例

次に、再配布された RIP ルート メトリックが EIGRP メトリックに変換される例を示します。使用する値は、次のとおりです。bandwidth = 1000、delay = 100、reliability = 250、loading = 100、および MTU = 1500。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 172.16.0.0
hostname(config-router)# redistribute rip
hostname(config-router)# default-metric 1000 100 250 100 1500
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成して、そのプロセスのルータ コンフィギュレーション モードを開始します。
redistribute（EIGRP）	EIGRP ルーティング プロセスにルートを再配布します。

delay

インターフェイスの遅延値を設定するには、インターフェイス コンフィギュレーション モードで **delay** コマンドを使用します。デフォルトの遅延値に戻すには、このコマンドの **no** 形式を使用します。

delay *delay-time*

no delay

構文の説明

delay-time	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。

デフォルト

デフォルトの遅延はインターフェイス タイプによって異なります。インターフェイスのデフォルト値を確認するには、**show interface** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

値は 10 マイクロ秒単位で入力します。**show interface** の出力に表示される遅延値は、マイクロ秒単位です。

例

次に、インターフェイスの遅延をデフォルトの 1000 から 2000 に変更する例を示します。**delay** コマンドの前と後に切り捨てられた **show interface** コマンドの出力が含まれ、このコマンドが遅延値にどのように影響を与えるかを示します。遅延値は、**show interface** の出力の 2 行め、DLY ラベルの後に記載されます。

遅延値を 2000 に変更するために入力するコマンドは、**delay 2000** ではなく **delay 200** です。これは、**delay** コマンドで入力する値が 10 マイクロ秒単位であり、**show interface** の出力ではマイクロ秒単位で表示されるためです。

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

```
hostname(config-if)# delay 200
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計情報および設定を表示します。

delete

ディスク パーティションのファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/noconfirm**] [**/recursive**] [**flash:**]*filename*

構文の説明

/noconfirm	（任意）確認のためのプロンプトを表示しないように指定します。
/recursive	（任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。
filename	削除するファイルの名前を指定します。
flash:	削除できない内部フラッシュを、コロンを付けて指定します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルの削除を実行すると、ファイル名のプロンプトが表示されるため、削除を確認する必要があります。

次の例は、現在の作業ディレクトリにある *test.cfg* という名前のファイルを削除する方法を示しています。

```
hostname# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny-message（グループ ポリシー webvpn コンフィギュレーション モード）

WebVPN に正常にログインした VPN 特権を持たないリモート ユーザに配信されたメッセージを変更するには、グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。リモート ユーザがメッセージを受信しないようにストリングを削除するには、このコマンドの **no** 形式を使用します。

deny-message value "*string***"**

no deny-message value

構文の説明

string	491 文字以下の英数字。特殊文字、スペース、および句読点を含みます。

デフォルト

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features.Contact your IT administrator for more information.」

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、トンネル グループ webvpn コンフィギュレーション モードからグループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **属性** を入力してから、**webvpn** コマンドを入力する必要があります（ポリシー *name* はすでに作成済みと見なされます）。

no deny-message none コマンドは、グループ webvp コンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

deny-message value コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

VPN セッションに使用されるトンネル ポリシーとは独立して、ログイン時にリモート ユーザのブラウザにテキストが表示されます。

例

次に、group2 という名前の内部グループ ポリシーを作成する最初のコマンドの例を示します。後続のコマンドによって、このポリシーに関連付けられている拒否メッセージを変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However, you have not been granted rights to use the VPN features. Contact your administrator for more information."
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
clear configure group-policy	すべてのグループ ポリシー コンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成します。
group-policy attributes	グループ ポリシー属性コンフィギュレーション モードを開始します。
show running-config group-policy [*name*]	指定したポリシーの実行グループ ポリシー コンフィギュレーションが表示されます。
webvpn（グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モード）	グループ ポリシー webvpn コンフィギュレーション モードを開始します。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。このモードには、グローバル コンフィギュレーション モードから **snmp-map** コマンドを入力してアクセスできます。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

deny version *version*

no deny version *version*

構文の説明

version	セキュリティ アプライアンスがドロップする SNMP トラフィックのバージョンを指定します。使用可能な値は、**1**、**2**、**2c**、および **3** です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SNMP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

SNMP トラフィックを特定の SNMP バージョンに制限するには、**deny version** コマンドを使用します。以前のバージョンの SNMP はセキュリティがより低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限できます。**deny version** コマンドは SNMP マップ内で使用します。SNMP マップは、**snmp-map** コマンドを使用して設定します。SNMP マップの作成後に、**inspect snmp** コマンドを使用してこのマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスに適用します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイス適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
```

```
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキスト、オブジェクト グループ、または DAP レコード）に対する説明を追加するには、各コンフィギュレーション モードで **description** コマンドを使用します。説明により、役立つ情報がコンフィギュレーションに追加されます。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

text	説明を最大 200 文字のテキスト ストリングで設定します。ダイナミック アクセス ポリシー レコード モードの場合、最大長は 80 文字です。 ストリングに疑問符（?）を含める場合は、不注意から CLI ヘルプを呼び出さないように、Ctrl+V を入力してから疑問符を入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

このコマンドは、さまざまなコンフィギュレーション モードで使用できます。

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	ダイナミック アクセス ポリシー レコード モードのサポートが追加されました。

例

次に、「管理」コンテキスト コンフィギュレーションに説明を追加する例を示します。

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドのアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
gtp-map	GTP インスペクション エンジンのパラメータを制御します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定したトラフィックに適用するアクションを指定します。

dhcp client route distance

DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dhcp client route distance *distance*

no dhcp client route distance *distance*

構文の説明

distance	DHCP を通じて学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

デフォルト

DHCP を通じて学習したルートには、デフォルトでアドミニストレーティブ ディスタンス 1 が指定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route distance コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP を通じて学習された後に **dhcp client route distance** コマンドが開始されると、指定したアドミニストレーティブ ディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route track	DHCP を通じて学習したルートをトラッキング エントリ オブジェクトに関連付けます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように DHCP クライアントを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route track** コマンドを使用します。DHCP クライアントのルート トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcp client route track *number*

no dhcp client route track

構文の説明

number	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route track コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP から学習された後で **dhcp client route track** コマンドを入力すると、学習された既存のルートはトラッキング オブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
```

```
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route distance	DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを割り当てます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp-client broadcast-flag

セキュリティ アプライアンスによる DHCP クライアント パケットへのブロードキャスト フラグの設定を許可するには、グローバル コンフィギュレーション モードで **dhcp-client broadcast-flag** コマンドを使用します。ブロードキャスト フラグを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ブロードキャスト フラグはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、DHCP クライアントが検出を送信して IP アドレスを要求するときに、このコマンドを使用して、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定できます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

no dhcp-client broadcast-flag コマンドを入力すると、ブロードキャスト フラグは 0 に設定され、DHCP サーバは応答パケットを提供された IP アドレスのクライアントにユニキャストします。

DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

例

次に、ブロードキャスト フラグをイネーブルにする例を示します。

```
hostname(config)# dhcp-client broadcast-flag
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。

interface	IP アドレスを設定するために、インターフェイス コンフィギュレーション モードを開始します。
dhcp-client client-id	DHCP 要求パケット オプション 61 を、インターフェイス MAC アドレスが含まれるように設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp-client client-id

デフォルトの内部生成ストリングではなく、オプション 61 の DHCP 要求パケットに MAC アドレスが保存されるよう強制するには、グローバル コンフィギュレーション モードで **dhcp-client client-id** コマンドを使用します。MAC アドレスを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

構文の説明

interface *interface_name*	オプション 61 用に MAC アドレスをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトでは、オプション 61 には内部生成 ASCII ストリングが使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、一部の ISP でオプション 61 がインターフェイス MAC アドレスであると見なされます。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。**dhcp-client client-id** コマンドを使用して、オプション 61 用にインターフェイス MAC アドレスを含めます。

例

次に、外部インターフェイスのオプション 61 用に MAC アドレスをイネーブルに例を示します。

```
hostname(config)# dhcp-client client-id interface outside
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。
interface	IP アドレスを設定するために、インターフェイス コンフィギュレーション モードを開始します。

dhcp-client broadcast-flag	DHCP クライアント パケットにブロードキャスト フラグを設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp-client update dns

DHCP クライアントが DHCP サーバに渡す更新パラメータを設定するには、グローバル コンフィギュレーション モードで **dhcp-client update dns** コマンドを使用します。DHCP クライアントが DHCP サーバに渡すパラメータを削除するには、このコマンドの **no** 形式を使用します。

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

構文の説明

both	DHCP サーバが DNS A および PTR リソース レコードの両方を更新するクライアント要求。
none	DHCP サーバが DDNS 更新を実行しないクライアント要求。
server	DHCP サーバがクライアント要求を受信するように指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、DHCP サーバが PTR RR 更新のみを実行するよう要求します。クライアントはサーバに FQDN オプションを送信しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはインターフェイス コンフィギュレーション モードでも入力できますが、ハイフンは使用しません。「**dhcp client update dns**」を参照してください。インターフェイス モードで **dhcp client update dns** コマンドを入力すると、グローバル コンフィギュレーション モードのこのコマンドで設定した設定値が上書きされます。

例

次に、DHCP サーバが A および PTR RR を更新しないことを要求するようクライアントを設定する例を示します。

```
hostname(config)# dhcp-client update dns server none
```

次に、サーバが A および PTR RR を更新することを要求するようクライアントを設定する例を示します。

```
hostname(config)# dhcp-client update dns server both
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp client update dns	
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcp-network-scope

セキュリティ アプライアンス DHCP サーバが、このグループ ポリシーのユーザにアドレスを割り当てるために使用する必要がある IP アドレスの範囲を指定するには、グループ ポリシー コンフィギュレーション モードで **dhcp-network-scope** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。値を継承できないようにするには、**dhcp-network-scope none** コマンドを使用します。

dhcp-network-scope {*ip_address*} | none

no dhcp-network-scope

構文の説明

ip_address	このポリシー グループのユーザに IP アドレスを割り当てるため、DHCP サーバが使用する必要がある IP サブネットワークを指定します。
none	DHCP サブネットワークをヌル値に設定して、IP アドレスが許可されないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、First Group という名前のグループ ポリシーに対して、IP サブネットワーク 10.10.85.0 を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

dhcp-server

VPN トンネルの確立時にクライアントに IP アドレスを割り当てる DHCP サーバのサポートを設定するには、トンネル グループ一般属性コンフィギュレーション モードで **dhcp-server** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

[no] dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

構文の説明

<ip1>	DHCP サーバのアドレス。
<ip2>-<ip10>	（任意）追加の DHCP サーバ。 1 回のコマンドで最大 10 個まで指定できます。また、複数のコマンドにまたがって指定できます。
link-selection	（任意）セキュリティ アプライアンスが RFC 3527 で定義されている DHCP サブ オプション 5（リレー情報オプション 82 のリンク選択のサブオプション）を送信するかどうかを指定するための設定。この設定は、この RFC をサポートするサーバでのみ使用してください。
subnet-selection	（任意）セキュリティ アプライアンスが RFC 3011 で定義されている DHCP オプション 118（IPv4 サブネットの選択のオプション）を送信するかどうかを指定するための設定。この設定は、この RFC をサポートするサーバでのみ使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(5)	link-selection オプションおよび subnet-selection オプションを追加しました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。

例

次のコマンドを config-general コンフィギュレーション モードで入力して、3 つの DHCP サーバ（dhcp1、dhcp2、および dhcp3）を IPSec リモートアクセス トンネル グループ「remotegrp」に追加する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

（注） プールのサイズは、Cisco ASA 5505 のユーザ ライセンス数が 10 の場合は 32 アドレス、Cisco ASA 5505 のユーザ ライセンス数が 50 の場合は 128 アドレスにそれぞれ制限されます。Cisco ASA 5505 のユーザ ライセンスが無制限の場合、およびその他すべてのセキュリティ アプライアンス プラットフォーム上では、256 アドレスがサポートされます。

構文の説明

interface_name	アドレス プールの割り当て先のインターフェイス。
IP_address1	DHCP アドレス プールの開始アドレス。
IP_address2	DHCP アドレス プールの終了アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd address *ip1*[*-ip2*] *interface_name* コマンドは、DHCP サーバのアドレス プールを指定します。セキュリティ アプライアンス DHCP サーバのアドレス プールは、そのアドレス プールがイネーブルなセキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があります。また、*interface_name* を使用して関連するセキュリティ アプライアンス インターフェイスを指定する必要があります。

アドレス プールのサイズは、セキュリティ アプライアンスでプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、セキュリティ アプライアンス インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的にセキュリティ アプライアンス DHCP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」（ダッシュ）文字がオブジェクト名の一部ではなく、範囲指定子と解釈されるため、「-」文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用して、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

次に、内部インターフェイスに DHCP サーバを設定する例を示します。その内部インターフェイスの DHCP サーバに IP アドレス 10 個のプールを割り当てるため、**dhcpd address** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP または PPPoE クライアントを実行しているインターフェイスから取得した値に基づいて、セキュリティ アプライアンスが DHCP サーバに対して DNS、WINS およびドメイン名の値を自動的に設定するのをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

構文の説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。
interface *if_name*	アクションが適用されるインターフェイスを指定します。
vpnclient-wins-override	vpnclient パラメータにより、インターフェイス DHCP または PPPoE クライアントの WINS パラメータを上書きします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータで上書きされます。

例

次に、内部インターフェイスに DHCP を設定する例を示します。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには、**dhcpd auto_config** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd auto_config outside
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。定義されたサーバをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns [*dnsip1* [*dnsip2*]] [**interface** *if_name*]

構文の説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレス。
dnsip2	（任意）DHCP クライアントの代替 DNS サーバの IP アドレス。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd dns コマンドは、DHCP クライアントに対する DNS サーバの IP アドレスを 1 つまたは複数指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次に、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用して、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。DNS ドメイン名をクリアするには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

構文の説明

domain_name	example.com などの DNS ドメイン名。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次に、**dhcpd domain** コマンドを使用して、セキュリティ アプライアンスで DHCP サーバにより DHCP クライアントに提供されるドメイン名を設定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd enable** コマンドを使用します。DHCP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。DHCP サーバは、DHCP クライアントにネットワーク コンフィギュレーション パラメータを提供します。セキュリティ アプライアンス内で DHCP サーバをサポートすることにより、セキュリティ アプライアンスは DHCP を使用して接続されるクライアントを設定できるようになります。

dhcpd enable *interface*

no dhcpd enable *interface*

構文の説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd enable *interface* コマンドを使用すると、DHCP デーモンによる、DHCP 対応のインターフェイス上での DHCP クライアントの要求のリッスンをイネーブルにできます。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

（注）　マルチ コンテキスト モードの場合は、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

セキュリティ アプライアンスが DHCP クライアント要求に応答する場合、要求を受信したインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注）　セキュリティ アプライアンス DHCP サーバ デーモンは、直接セキュリティ アプライアンス インターフェイスに接続されていないクライアントはサポートしません。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、**dhcpd enable** コマンドを使用して、DHCP サーバを内部インターフェイス上でイネーブルにする例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバのデバッグ情報を表示します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
lease_length	DHCP サーバから DHCP クライアントに与えられる、秒単位の IP アドレスのリース期間。有効な値は、300 ～ 1048575 秒です。

デフォルト

lease_length のデフォルト値は 3600 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd lease コマンドは、DHCP クライアントに与えるリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース期間を削除して、この値をデフォルト値の 3600 秒に置き換えます。

例

次に、**dhcpd lease** コマンドを使用して、DHCP クライアントに対する DHCP 情報のリース期間を指定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプションを設定するには、グローバル コンフィギュレーション モードで **dhcpd option** コマンドを使用します。オプションをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

構文の説明

ascii	オプション パラメータが ASCII 文字ストリングであることを指定します。
code	設定された DHCP オプションの番号。有効な値は、0 ～ 255 であり、いくつかの例外があります。サポートされていない DHCP オプション コードのリストについては、下の使用上のガイドラインを参照してください。
hex	オプション パラメータが 16 進ストリングであることを指定します。
hex_string	16 進ストリングをスペースのない偶数桁で指定します。0x プレフィックスを使用する必要はありません。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを **ip** キーワードに指定できます。
IP_address	ドット付き 10 進表記の IP アドレスを指定します。
string	スペースなしの ASCII 文字ストリングを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd option コマンドを使用して、TFTP サーバ情報を Cisco IP Phone およびルータに提供することができます。

DHCP オプション要求がセキュリティ アプライアンス DHCP サーバに到着すると、セキュリティ アプライアンスは **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 コマンドおよび **dhcpd option 150** コマンドは、Cisco IP Phone およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。次のようにコマンドを使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は TFTP サーバの IP アドレスまたはホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

（注）　**dhcpd option 66** コマンドは **ascii** パラメータのみ受け付け、**dhcpd option 150** コマンドは **ip** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信ルールが適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、および **access-list** エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の着信ルールが適用されます。TFTP サーバ用のスタティック ステートメントと **access-list** ステートメントのグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC2132 を参照してください。

（注）　セキュリティ アプライアンスは、与えられたオプション タイプおよび値が RFC 2132 に規定されているオプション コードの想定タイプおよび想定値と一致していることを確認しません。たとえば、**dhcpd option 46 ascii hello** と入力した場合、セキュリティ アプライアンスはその設定を受け入れますが、オプション 46 は 1 桁の 16 進値が想定されるとして RFC 2132 に規定されます。

dhcpd option コマンドで次の DHCP オプションは設定できません。

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER

オプション コード	説明
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次に、DHCP オプション 66 に TFTP サーバを指定する例を示します。

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP ping のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをアドレスに送信します。このコマンドは、ping タイムアウトをミリ秒で指定します。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
number	ミリ秒単位の ping タイムアウト値。最小値は 10、最大値は 10000 です。デフォルト値は 50 です。

デフォルト

number のデフォルトのミリ秒は 50 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP ping パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、セキュリティ アプライアンスは IP アドレスを割り当てる前に、1500 ミリ秒（各 ICMP ping パケットに対して 750 ミリ秒）待ちます。

ping のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次に、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの ping タイムアウト値を変更する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
```

```
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd update dns

DHCP サーバによるダイナミック DNS 更新の実行をイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd update dns** コマンドを使用します。DHCP サーバによる DDNS をディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

構文の説明

both	DHCP サーバが A と PTR の両方の DNS RR を更新するように指定します。
interface	DDNS 更新が適用されるセキュリティ アプライアンス インターフェイスを指定します。
override	DHCP サーバが DHCP クライアント要求を上書きするように指定します。
srv_ifc_name	このオプションを適用するインターフェイスを指定します。

デフォルト

デフォルトでは、DHCP サーバは PTR RR 更新のみを実行します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。更新は DHCP サーバと連携して実行されます。**dhcpd update dns** コマンドはサーバによる更新をイネーブルにします。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方の更新、または PTR RR 更新のみを実行するように設定できます。DHCP クライアントからの更新要求を上書きするように設定することもできます。

例

次に、DDNS サーバが DHCP クライアントからの要求を上書きすると同時に、A と PTR の両方の更新を実行するよう設定する例を示します。

```
hostname(config)# dhcpd update dns both override
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	DDNS アップデート方式をセキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd wins

DHCP クライアントに対して WINS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd wins** コマンドを使用します。WINS サーバを DHCP サーバから削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（任意）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcpd wins コマンドは、DHCP クライアント用の WINS サーバのアドレスを指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次に、dhcpd wins コマンドを使用して、DHCP クライアントに送信された WINS サーバ情報を指定する例を示します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェントをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcprelay enable** コマンドを使用します。DHCP リレー エージェントをディセーブルにするには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントでは、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

構文の説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイスの名前。

デフォルト

DHCP リレー エージェントはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスが **dhcprelay enable** *interface_name* コマンドを使用して DHCP リレー エージェントを開始するには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。このコマンドがない場合、セキュリティ アプライアンスは次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。
- 1 つのコンテキスト上で、DHCP リレーを DHCP サーバと同時にイネーブルにすることはできません。

- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次に、DHCP リレー エージェントをディセーブルにする例を示します。

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントのデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server

DHCP 要求が転送される DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP サーバを DHCP リレー コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントでは、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address* [*interface_name*]

構文の説明

interface_name	DHCP サーバが常駐するセキュリティ アプライアンス インターフェイスの名前。
IP_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP サーバの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できますが、セキュリティ アプライアンスに設定できる DHCP リレー サーバは 10 までという制限があります。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドをセキュリティ アプライアンス コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、インターフェイスは DHCP パケットのそのサーバへの転送を停止します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、*IP_address* [*interface_name*] で指定された DHCP サーバ用の DHCP リレー エージェント コンフィギュレーションだけが削除されます。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト ルータを削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定されたセキュリティ アプライアンス インターフェイスのアドレスに置き換えられます。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

構文の説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcprelay setroute *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがない場合、セキュリティ アプライアンスは *interface* アドレスを含むデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートがセキュリティ アプライアンスに向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないままセキュリティ アプライアンスを通過します。

例

次に、**dhcprelay setroute** コマンドを使用して、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバからセキュリティ アプライアンスの内部インターフェイスに設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
```

```
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcprelay timeout *seconds*

no dhcprelay timeout

構文の説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

dhcprelay タイムアウトのデフォルト値は 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間を秒単位で設定します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイスに設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dialog

WebVPN ユーザに表示するダイアログ メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **dialog** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

構文の説明

border	境界を変更することを指定します。
message	メッセージを変更することを指定します。
style	スタイルを変更することを指定します。
title	タイトルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または CSS パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのスタイルは background-color:#669999;color:white です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:black です。

デフォルトの境界線のスタイルは border:1px solid black;border-collapse:collapse です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。

- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ダイアログ メッセージの文字表示色を青色に変更するようにカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# dialog message style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir [/all] [**all-filesystems**] [**/recursive**] [**flash:** | **system:**] [*path]*

構文の説明

/all	（任意）すべてのファイルを表示します。
all-filesystems	（任意）すべてのファイルシステムのファイルを表示します。
disk0:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
/recursive	（任意）ディレクトリの内容を再帰的に表示します。
system:	（任意）ファイル システムのディレクトリの内容を表示します。
flash:	（任意）デフォルトのフラッシュ パーティションのディレクトリ内容を表示します。
path	（任意）特定のパスを指定します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次に、ディレクトリの内容を表示する例を示します。

```
hostname# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、ファイル システム全体の内容を再帰的に表示する例を示します。

```
hostname# dir /recursive disk0:
Directory of disk0:/*
```

```
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

disable

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

enable コマンドを使用して、特権モードを開始します。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

例

次の例は、特権モードを開始する方法を示しています。

```
hostname> enable
hostname#
```

次に、特権モードを終了する例を示します。

```
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードをイネーブルにします。

disable（キャッシュ）

WebVPN に対するキャッシングをディセーブルにするには、キャッシュ コンフィギュレーション モードで **disable** コマンドを使用します。キャッシングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。

disable

no disable

デフォルト

キャッシングは、各キャッシュ属性に対するデフォルトの設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシングをディセーブルにしてから、それを再度イネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# disable
hostname(config-webvpn-cache)# no disable
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。

コマンド	説明
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

disable service-settings

電話プロキシ機能の使用時に IP 電話のサービス設定をディセーブルにするには、電話プロキシ コンフィギュレーション モードで **disable service-settings** コマンドを使用します。IP 電話の設定を保持するには、このコマンドの **no** 形式を使用します。

disable service-settings

no disable service-settings

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

サービス設定はデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、次の設定内容が IP 電話ではディセーブルになります。

- PC ポート
- Gratuitous ARP
- Voice VLAN アクセス
- Web アクセス
- Span to PC Port

設定されている各 IP フォンの CUCM で設定されている設定を保持するには、**no disable service-settings** コマンドを設定します。

例

次に、**disable service-settings** コマンドを使用して、ASA で電話プロキシ機能を使用する IP 電話の設定を保持する例を示します。

```
hostname(config-phone-proxy)# no disable service-settings
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show phone-proxy	Phone Proxy 固有の情報を表示します。

display

セキュリティ アプライアンスが DAP 属性データベースに書き込む属性値のペアを表示するには、DAP テスト属性モードで **display** コマンドを入力します。

display

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP テスト属性	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。**display** コマンドを使用すると、これらの属性をコンソールに表示できます。

関連コマンド

コマンド	説明
attributes	属性モードを開始します。このモードでは属性値のペアを設定できます。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセス ポリシーをコンソールに表示します。

distance eigrp

内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定するには、ルータ コンフィギュレーション モードで **distance eigrp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance eigrp *internal-distance external-distance*

no distance eigrp

構文の説明

external-distance	EIGRP 外部ルートのアドミニストレーティブ ディスタンス。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効な値は、1 ～ 255 です。
internal-distance	EIGRP 内部ルートのアドミニストレーティブ ディスタンス。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。

デフォルト

デフォルト値は次のとおりです。

- *external-distance* は 170 です。
- *internal-distance* は 90 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に複数の異なるルートがある場合に、セキュリティ アプライアンスが最適なパスの選択に使用するルート パラメータです。

セキュリティ アプライアンスで複数のルーティング プロトコルが実行されている場合、**distance eigrp** コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。表 11-1 に、セキュリティ アプライアンスでサポートされているルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンスを示します。

表 11-1　デフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP 集約ルート	5
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
不明	255

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、内部と外部の両方の EIGRP ルートのアドミニストレーティブ ディスタンスがデフォルトに戻されます。

例

次に、**distance eigrp** コマンドを使用して、すべての EIGRP 内部ルートのアドミニストレーティブ ディスタンスを 80 に、すべての EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定する例を示します。EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定すると、EIGRP によって検出されたルートが、RIP（OSPF ではなく）によって検出された同じルートを経由する特定の宛先設定に渡されます。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.7.0
hostname(config-router)# network 172.16.0.0
hostname(config-router)# distance eigrp 90 115
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

distance ospf

ルート タイプに基づいて OSPF ルートのアドミニストレーティブ ディスタンスを定義するには、ルータ コンフィギュレーション モードで **distance ospf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

構文の説明

d1、*d2*、*d3*	各ルート タイプの距離。有効値の範囲は、1 ～ 255 です。
external	（任意）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（任意）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（任意）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

少なくとも 1 つのキーワードと引数を指定する必要があります。アドミニストレーティブ ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。アドミニストレーティブ ディスタンスを再入力する場合、対象ルート タイプのアドミニストレーティブ ディスタンスだけが変更されます。その他のルート タイプのアドミニストレーティブ ディスタンスは影響されません。

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、すべてのルート タイプのアドミニストレーティブ ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルート タイプをデフォルトのアドミニストレーティブ ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- コマンドの **no** 形式を使用してコンフィギュレーション全体を削除してから、保持するルート タイプのコンフィギュレーションを再入力します。

例

次に、外部ルートのアドミニストレーティブ ディスタンスを 150 に設定する例を示します。

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

次に、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される例を示します。

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

次に、各アドミニストレーティブ ディスタンスを 105 に設定し、次に外部アドミニストレーティブ ディスタンスのみを 150 に変更する例を示します。**show running-config router ospf** コマンドは、外部ルート タイプの値だけが変更され、その他のルート タイプでは以前に設定された値が保持されている状況を示します。

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list in

ルーティング アップデートで受信するネットワークをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

構文の説明

acl	標準アクセス リスト名。
if_name	（任意）**nameif** コマンドで指定したインターフェイス名。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

着信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する RIP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
hostname(config)# access-list ripfilter permit 10.0.0.0
hostname(config)# access-list ripfilter deny any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter in interface outside
```

次に、外部インターフェイスで受信する EIGRP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
hostname(config)# access-list eigrp_filter permit 10.0.0.0
hostname(config)# access-list eigrp_filter deny any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
```

```
hostname(config-router)# distribute-list eigrp_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list out	ルーティング アップデートでアドバタイズされるネットワークをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list out

ルーティング アップデートで送信される特定のネットワークをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

構文の説明

acl	標準アクセス リスト名。
connected	（任意）接続されたルートのみフィルタリングします。
eigrp *as_number*	（任意）指定した自律システム番号からの EIGRP ルートだけをフィルタリングします。*as_number* は、セキュリティ アプライアンス上の EIGRP ルーティング プロセスの自律システム番号です。
interface *if_name*	（任意）**nameif** コマンドで指定したインターフェイス名。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスに送信されたルーティング アップデートにのみ適用されます。
ospf *pid*	（任意）指定した OSPF プロセスにより検出された OSPF ルートのみフィルタリングします。
rip	（任意）RIP ルートのみフィルタリングします。
static	（任意）スタティック ルートのみフィルタリングします。

デフォルト

送信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	**eigrp** キーワードが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての発信更新に適用されます。

例

次に、任意のインターフェイスから送信された RIP 更新で 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
hostname(config)# access-list ripfilter deny 10.0.0.0
hostname(config)# access-list ripfilter permit any
```

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter out
```

次に、EIGRP ルーティング プロセスで外部インターフェイスの 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
hostname(config)# access-list eigrp_filter deny 10.0.0.0
hostname(config)# access-list eigrp_filter permit any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list eigrp_filter out interface outside
```

関連コマンド

コマンド	説明
distribute-list in	ルーティング アップデートで受信するネットワークをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

dns domain-lookup

サポートされているコマンドに対してネーム ルックアップを実行するために、セキュリティ アプライアンスが DNS サーバに DNS 要求を送信することをイネーブルにするには、グローバル コンフィギュレーション モードで **dns domain-lookup** コマンドを使用します。DNS ルックアップをディセーブルにするには、このコマンドの **no** 形式を使用します。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

構文の説明

interface_name	DNS ルックアップをイネーブルにするインターフェイスを指定します。このコマンドを複数回入力して、DNS ルックアップを複数のインターフェイス上でイネーブルにする場合、セキュリティ アプライアンスは応答を受信するまで各インターフェイスを順番に試します。

デフォルト

デフォルトでは、DNS ルックアップはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

DNS 要求の送信先の DNS サーバ アドレスを設定するには、**dns name-server** コマンドを使用します。DNS ルックアップをサポートするコマンドのリストについては、**dns name-server** コマンドを参照してください。

セキュリティ アプライアンスは、ダイナミックに学習されたエントリで構成される名前解決のキャッシュを管理します。セキュリティ アプライアンスは、ホスト名から IP アドレスへの変換が必要になるたびに外部 DNS サーバにクエリーする代わりに、外部 DNS 要求から返された情報をキャッシュします。セキュリティ アプライアンスは、キャッシュにない名前に対してのみ要求を実行します。キャッシュのエントリは、DNS レコードの期限切れ、または 72 時間後のいずれか早い方に自動的にタイムアウトします。

例

次に、内部インターフェイス上で DNS ルックアップをイネーブルにする例を示します。

```
hostname(config)# dns domain-lookup inside
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-group（トンネル グループ webvpn コンフィギュレーション モード）

WebVPN トンネル グループに使用する DNS サーバを指定するには、トンネル グループ webvpn コンフィギュレーション モードで **dns-group** コマンドを使用します。デフォルトの DNS グループに戻すには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

構文の説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

名前には、任意の DNS グループを指定できます。dns-group コマンドはホスト名をトンネル グループの適切な DNS サーバに解決します。

dns server-group コマンドを使用して、DNS グループを設定します。

例

次に、「dnsgroup1」という名前の DNS グループの使用を指定するカスタマイゼーション コマンドの例を示します。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group dnsgroup1
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

dns-guard

クエリーごとに 1 つの DNS 応答を実行する DNS Guard 機能をイネーブルにするには、パラメータ コンフィギュレーション モードで **dns-guard** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

dns-guard

no dns-guard

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

DNS Guard は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no dns-guard** を明示的に指定する必要があります。**inspect dns** が設定されていない場合、動作は **global dns-guard** コマンドにより指定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ヘッダーの ID フィールドを使用して、DNS 応答と DNS ヘッダーを一致させます。クエリーごとに 1 つの応答がセキュリティ アプライアンスを介して許可されます。

例

次に、DNS インスペクション ポリシー マップで DNS Guard をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dns retries

セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dns retries *number*

no dns retries [*number*]

構文の説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトの再試行回数は 2 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、WebVPN 接続に対して廃止されました。

使用上のガイドライン

dns name-server コマンドを使用して DNS サーバを追加します。

例

次に、再試行回数を 0 回に設定する例を示します。セキュリティ アプライアンス により行われる試行は、各サーバに対して 1 回だけです。

```
hostname(config)# dns retries 0
hostname(config)#
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-server

プライマリおよびセカンダリの DNS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **dns-server** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

dns-server {**value** *ip_address* [*ip_address*] | none}

no dns-server

構文の説明

none	dns サーバに、ヌル値を設定して DNS サーバを許可しません。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このオプションを使用すると、別のグループ ポリシーの DNS サーバを継承できます。サーバが継承されないようにするには、**dns-server none** コマンドを使用します。

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。複数のサーバを設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の DNS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

dns server-group

トンネル グループに使用する DNS サーバのドメイン名、ネーム サーバ、再試行回数、およびタイムアウトの値を指定できる DNS サーバ グループ モードを開始するには、グローバル コンフィギュレーション モードで **dns server-group** コマンドを使用します。特定の DNS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

dns server -group *name*

no dns server-group

構文の説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前には、任意の DNS グループを指定できます。**dns server-group** コマンドを使用して、DNS グループを設定します。

例

次に、「eval」という名前の DNS サーバ グループを設定する例を示します。

```
hostname(config)# dns server-group eval
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 192.168.10.10
hostname(config-dns-server-group)# retries 5
hostname(config-dns-server-group)# timeout 7
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns timeout

次の DNS サーバを試すまで待機する時間を指定するには、グローバル コンフィギュレーション モードで **dns timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

dns timeout *seconds*

no dns timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。試行回数を設定するには、**dns retries** コマンドを参照してください。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、タイムアウトを 1 秒に設定します。

```
hostname(config)# dns timeout 1
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

domain-name

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンス は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバを修飾子を持たない名前の「jupiter」に指定した場合、セキュリティ アプライアンスによって名前は「jupiter.example.com」に修飾されます。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを example.com に設定する例を示します。

```
hostname(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。

コマンド	説明
hostname	セキュリティ アプライアンスのホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

domain-name（dns サーバ グループ）

デフォルトのドメイン名を設定するには、DNS サーバ グループ コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンス は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバを修飾子を持たない名前の「jupiter」に指定した場合、セキュリティ アプライアンスによって名前は「jupiter.example.com」に修飾されます。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DNS サーバ グループ コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.1(1)	**dns domain-lookup** コマンドはこのコマンドに置き換えられて廃止されました。

使用上のガイドライン

マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを「dnsgroup1」の「example.com」に設定する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# domain-name example.com
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。

コマンド	説明
domain-name	デフォルトのドメイン名をグローバルに設定します。
show running-config dns-server group	現在の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

downgrade

オペレーティング システム ソフトウェア（ソフトウェア イメージ）の以前のバージョンにダウングレードするには、特権 EXEC モードで **downgrade** コマンドを使用します。

注意　PIX セキュリティ アプライアンスが現在 PIX Version 7.0 以降を実行している場合は、以前のバージョンのソフトウェアをロードしないでください。PIX Version 7.0 ファイル システムがインストールされている PIX セキュリティ アプライアンスに、モニタ モードからソフトウェア イメージをロードすることは、予測できない動作を発生させるため、サポートされていません。ダウングレード プロセスを簡単に行うために用意された、実行中の PIX Version 7.0 イメージから、**downgrade** コマンドを使用することを強くお勧めします。

downgrade *image_url* **[activation-key [flash** | *4-part_key* | *file***]] [config** *start_config_url***]**

構文の説明

4-part_key	（任意）イメージに書き込むための 4 分割アクティベーション キーを指定します。 5 分割キーを使用する場合、4 分割キーに戻ることにより失われる可能性がある機能のリストと共に、警告が生成されます。 システム フラッシュが再フォーマットまたは消去された場合、ダウングレード用のデフォルト キーは使用できなくなります。その場合、CLI はコマンドラインにアクティベーション キーを入力するように求めます。これは、**activation-key** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
activation-key	（任意）ダウングレードされたソフトウェア イメージで使用するアクティベーション キーを指定します。
config	（任意）スタートアップ コンフィギュレーション ファイルを指定します。
file	（任意）ダウングレード手順が完了した後で使用するパスまたは URL およびアクティベーション キー ファイルの名前を指定します。アップグレード プロセス中にフラッシュに保存されたファイルが、ソースのイメージ ファイルだった場合、このファイル内のアクティベーション キーがダウングレードで使用されます。
flash	（任意）5 分割アクティベーション キーを使用する前にデバイスで使用されていた 4 分割アクティベーション キーをフラッシュ メモリで検索するように指定します。これは、**activation-key** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
image_url	ダウングレードするソフトウェア イメージのパスまたは URL および名前を指定します。ソフトウェア イメージは 7.0 の前のバージョンである必要があります。
start_config_url	（任意）ダウングレード手順が完了した後で使用するパスまたは URL およびコンフィギュレーション ファイルの名前を指定します。

デフォルト

activation-key キーワードが指定されていない場合、セキュリティ アプライアンスは最後に使用された 4 分割アクティベーション キーを試します。セキュリティ アプライアンスがフラッシュで 4 分割アクティベーション キーを検出できなかった場合、コマンドは拒否され、エラー メッセージが表示されます。この場合、次回にコマンドラインで有効な 4 分割アクティベーション キーを指定する必要があります。デフォルトのアクティベーション キーまたはユーザ指定のアクティベーション キーが、現在

有効なアクティベーション キーと比較されます。選択されたアクティベーション キーを使用することで、機能を損失する可能性がある場合、ダウングレード後に、損失する可能性のある機能のリストと共に警告が表示されます。

スタートアップ コンフィギュレーション ファイルが指定されていない場合、セキュリティ アプライアンスはデフォルトで downgrade.cfg を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•		

コマンド履歴

バージョン	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ソフトウェア バージョン 7.0 以降を実行している Cisco PIX Firewall シリーズのセキュリティ アプライアンスに限り使用できます。このコマンドは、Cisco ASA 5500 シリーズのセキュリティ アプライアンスではサポートされていません。

注意　ダウングレード プロセス中に電源障害が発生すると、フラッシュ メモリが破損する場合があります。予防策として、ダウングレード プロセスを開始する前に、フラッシュ メモリ上のすべてのデータを外部デバイスにバックアップしてください。

破損したフラッシュ メモリを回復するためには、コンソールへの直接アクセスが必要です。詳細については、**format** コマンドを参照してください。

例

次の例では、ソフトウェアをバージョン 6.3.3 にダウングレードします。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded







Rebooting....

Enter zero actkey:
```

次の例は、無効なアクティベーション キーを入力した場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
Error: activation key entered is invalid.

Enter the file option when there is no actkey in the source image (happens if the source
is in tftp server).
```

次の例は、ソース イメージのアクティベーション キーを指定したときに、それが存在しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

次の例は、最後のプロンプトでダウングレード手順を中止する方法を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

ダウングレードするには、ソフトウェア バージョンが 7.0 未満であることが必要です。次の例は、ソフトウェアのダウングレードに失敗した試行を示しています。

```
hostname# downgrade tftp://17.13.2.25//scratch/views/test/target/sw/cdisk
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

次の例は、イメージを指定したときにアクティベーション キーを確認しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

次の例は、4 分割アクティベーション キーに、現在の 5 分割アクティベーション キーのすべての機能が含まれていない場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

関連コマンド

コマンド	説明
copy running-config startup-config	現在の実行コンフィギュレーションをフラッシュ メモリに保存します。

download-max-size

ダウンロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **download-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

download-max-size <*size*>

no download-max-size

構文の説明

size	ダウンロードするオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

サイズを 0 に設定すると、実質的にオブジェクトのダウンロードは許可されません。

例

次に、ダウンロードするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# download-max-size 1500
```

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
upload-max-size	アップロードするオブジェクトの最大サイズを指定します。

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

drop

match コマンドまたは **class** コマンドと一致するパケットをすべてドロップするには、一致またはクラス コンフィギュレーション モードで drop コマンドを使用します。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットをドロップします。この drop アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop** コマンドを入力して **match** コマンドまたは **class** コマンドと一致するすべてのパケットをドロップできます。

パケットをドロップすると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションでパケットをドロップした場合は、それ以降、**match** コマンドまたは **class** コマンドと一致しません。最初のアクションがパケットのロギングである場合は、パケットのド

ロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

drop-connection

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop-connection** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラス マップと一致するトラフィックの接続を閉じます。接続は、セキュリティ アプライアンス上の接続データベースから削除されます。接続がドロップされたセキュリティ アプライアンスに入る後続パケットはすべて廃棄されます。この drop-connection アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop-connection** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を閉じます。

パケットをドロップするか、または接続を閉じると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションがパケットをドロップし接続を閉じることである場合、それ以降は **match** コマンドまたは **class** コマンドに対応しません。最初のアクションがパケッ

トのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop-connection** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、接続を閉じて、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dtls port

DTLS 接続用のポートを指定するには、webvpn コンフィギュレーション モードで **dtls port** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dtls port *number*

no dtls port *number*

構文の説明

number	UDP ポート番号（1 ～ 65535）。

デフォルト

デフォルトのポート番号は 443 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DTLS を使用する SSL VPN 接続用の UDP ポートを指定します。

DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

例

次に、webvpn コンフィギュレーション モードを開始し、DTLS 用にポート 444 を指定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# dtls port 444
```

関連コマンド

コマンド	説明
dtls enable	インターフェイスに対して DTLS をイネーブルにします。
svc dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	セキュリティ アプライアンスがリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

duplex

銅線イーサネット インターフェイス（RJ-45）のデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークで自動検出がサポートされていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックス方式を **auto** 以外に設定した場合は、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電源が供給されません。

例

次に、デュプレックス モードを全二重に設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

dynamic-access-policy-config

DAP レコードとそれに関連付けられたアクセス ポリシー属性を設定するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-config** コマンドを使用します。既存の DAP コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

DAP 選択コンフィギュレーション ファイルをアクティブにするには、activate 引数を指定して **dynamic-access-policy-config** コマンドを使用します。

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。
activate	DAP 選択コンフィギュレーション ファイルをアクティブにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
name：グローバル コンフィギュレーション activeate：特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで dynamic-access-policy-config コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- action
- description
- network-acl
- priority
- user-message
- webvpn

例

次に、user1 という名前の DAP レコードを設定する例を示します。

```
hostname(config)# dynamic-access-policy-config user1
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードにアクセス ポリシー属性を入力します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

dynamic-access-policy-record

DAP レコードを作成してアクセス ポリシー属性を入力するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用します。既存の DAP レコードを削除するには、このコマンドの **no** 形式を使用します。

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで dynamic-access-policy-record コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- action
- description
- network-acl
- priority
- user-message
- webvpn

例

次に、Finance という名前の DAP レコードを作成する例を示します。

```
hostname(config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
clear config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定された DAP レコードを削除します。
dynamic-access-policy-config url	DAP 選択コンフィギュレーション ファイルを設定します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

CHAPTER 12

eigrp log-neighbor-changes コマンド～ functions（removed）コマンド

eigrp log-neighbor-changes

EIGRP ネイバーとの隣接関係の変更のロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp log-neighbor-changes コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの変更のロギングをディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-changes
```

関連コマンド

コマンド	説明
eigrp log-neighbor-warnings	ネイバー警告メッセージのロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp log-neighbor-warnings

EIGRP ネイバー警告メッセージのロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

構文の説明

seconds	（任意）ネイバー警告メッセージの反復間隔（秒数）。有効な値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。すべてのネイバー警告メッセージがログに記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp log-neighbor-warnings コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの警告メッセージのロギングをディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-warnings
```

次に、EIGRP ネイバー警告メッセージをログに記録し、5 分（300 秒）間隔で警告メッセージを繰り返す例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp log-neighbor-warnings 300
```

関連コマンド

コマンド	説明
eigrp log-neighbor-messages	EIGRP ネイバーとの隣接関係に関する変更のロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp router-id

EIGRP ルーティング プロセスによって使用されるルータ ID を指定するには、ルータ コンフィギュレーション モードで **eigrp router-id** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

構文の説明

ip-addr	IP アドレス形式（ドット付き 10 進形式）でのルータ ID。ルータ ID として 0.0.0.0 または 255.255.255.255 を使用することはできません。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp router-id コマンドが設定されていない場合、EIGRP では、EIGRP プロセスの開始時に、セキュリティ アプライアンス上で最大の IP アドレスが自動的に選択されて、ルータ ID として使用されます。**no router eigrp** コマンドを使用して EIGRP プロセスを削除するか、または **eigrp router-id** コマンドを使用して手動でルータ ID を設定しない限り、ルータ ID は変更されません。

ルータ ID は、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。このような事態を回避するには、**eigrp router-id** コマンドを使用して、ルータ ID のグローバル アドレスを指定します。

各 EIGRP ルータには、一意の値を設定する必要があります。

例

次に、EIGRP ルーティング プロセスの固定ルータ ID として 172.16.1.3 を設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp router-id 172.16.1.3
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp stub

EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定するには、ルータ コンフィギュレーション モードで **eigrp stub** コマンドを使用します。EIGRP スタブ ルーティングを削除するには、このコマンドの **no** 形式を使用します。

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [receive-only] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

構文の説明

connected	（任意）接続ルートをアドバタイズします。
receive-only	（任意）セキュリティ アプライアンスを受信専用ネイバーとして設定します。
redistributed	（任意）他のルーティング プロトコルから再配布されたルートをアドバタイズします。
static	（任意）スタティック ルートをアドバタイズします。
summary	（任意）集約ルートをアドバタイズします。

デフォルト

スタブ ルーティングはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp stub コマンドを使用して、セキュリティ アプライアンスをスタブとして設定します。この場合、セキュリティ アプライアンスでは、すべての IP トラフィックがディストリビューション ルータに転送されます。

receive-only キーワードを使用すると、セキュリティ アプライアンスが自律システム内の他のどのルータともルートを共有しないように設定できます。セキュリティ アプライアンスは、EIGRP ネイバーからの更新のみを受信します。**receive-only** キーワードは他のキーワードと組み合わせて使用することはできません。

connected、**static**、**summary**、および **redistributed** の各キーワードは、1 つ以上を組み合わせて指定できます。これらのいずれかのキーワードを指定して **eigrp stub** コマンドを使用した場合、これらの特定のキーワードによって指定されたルート タイプのみが送信されます。

connected キーワードを指定すると、EIGRP スタブ ルーティング プロセスで接続ルートを送信できます。接続ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用して接続ルートの再配布が必要となることがあります。

static キーワードを指定すると、EIGRP スタブ ルーティング プロセスでスタティック ルートを送信できます。このオプションを設定しない場合、EIGRP ではスタティック ルートは送信されません。スタティック ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用してスタティック ルートの再配布が必要となることがあります。

summary キーワードを指定すると、EIGRP スタブ ルーティング プロセスで集約ルートを送信できます。集約ルートは、**summary-address eigrp** コマンドを使用して手動で作成することも、**auto-summary** コマンドをイネーブルにして自動的に作成することもできます（**auto-summary** はデフォルトでイネーブルになっています）。

redistributed キーワードを指定すると、EIGRP スタブ ルーティング プロセスで、他のルーティング プロトコルから EIGRP ルーティング プロセスに再配布されたルートを送信できます。このオプションを設定しない場合、再配布されたルートは EIGRP によってアドバタイズされません。

例

次に、**eigrp stub** コマンドを使用して、接続ルートおよび集約ルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected summary
```

次に、**eigrp stub** コマンドを使用して、接続ルートおよびスタティック ルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。集約ルートの送信は許可されません。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected static
```

次に、**eigrp stub** コマンドを使用して、EIGRP 更新の受信のみを行う EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。接続ルート、集約ルート、およびスタティック ルートの情報は送信されません。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 eigrp
hostname(config-router)# eigrp stub receive-only
```

次に、**eigrp stub** コマンドを使用して、他のルーティング プロトコルから EIGRP に再配布されたルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub redistributed
```

次に、オプションの引数を指定しないで **eigrp stub** コマンドを使用する例を示します。引数なしで **eigrp stub** コマンドを使用すると、デフォルトで接続ルートおよびスタティック ルートがアドバタイズされます。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub
```

関連コマンド

コマンド	説明
router eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

eject

ASA 5500 シリーズの外部コンパクト フラッシュ デバイスの取り外しをサポートするには、ユーザ EXEC モードで **eject** コマンドを使用します。

eject [*/noconfirm*] *disk1:*

構文の説明

disk1:	取り外すデバイスを指定します。
/noconfirm	セキュリティ アプライアンスから外部フラッシュ デバイスを物理的に取り外す前に、デバイスを取り外すかどうかの確認が必要ないことを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eject コマンドを使用すると、ASA 5500 シリーズ セキュリティ アプライアンスからコンパクト フラッシュ デバイスを安全に取り外すことができます。

次に、**eject** コマンドを使用して、デバイスをセキュリティ アプライアンスから物理的に取り外す前に *disk1* を正常にシャットダウンする例を示します。

```
hostname# eject /noconfig disk1:
It is now safe to remove disk1:
hostname# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

email

登録時に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **email** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

email *address*

no email

構文の説明

address	電子メール アドレスを指定します。*address* の最大長は 64 文字です。

デフォルト

デフォルト設定は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•		

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に電子メール アドレス user1@user.net を含める例を示します。

```
hostname(config)# crypto ca-trustpoint central
hostname(ca-trustpoint)# email user1@user.net
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca-trustpoint	トラストポイント コンフィギュレーション モードを開始します。

enable

特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

構文の説明

level	（任意）0 ～ 15 の特権レベル。enable 認証（**aaa authentication enable console** コマンド）では使用されません。

デフォルト

enable 認証（**aaa authentication enable console** コマンドを使用）を使用していない場合は、特権レベル 15 を開始します。enable 認証の場合、デフォルトのレベルは、ユーザ名に設定されているレベルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デフォルトのイネーブル パスワードはブランクです。パスワードの設定については、**enable password** コマンドを参照してください。

enable 認証を使用しない場合は、**enable** コマンドを入力すると、ユーザ名が enable_*level* に変更されます。デフォルトのレベルは 15 です。enable 認証を使用する場合（**aaa authentication enable console** コマンドを使用）、ユーザ名および関連するレベルは維持されます。ユーザ名の維持は、コマンド認可（ローカルまたは TACACS+ を使用した **aaa authorization command** コマンド）で重要です。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。中間のレベルを使用するには、ローカル コマンド認可（**aaa authorization command LOCAL** コマンド）をイネーブルにし、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。TACACS+ コマンド認可では、セキュリティ アプライアンスに設定された特権レベルは使用されません。

現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

特権 EXEC モードを終了するには、**disable** コマンドを入力します。

例

次に、特権 EXEC モードを開始する例を示します。

```
hostname> enable
Password: Pa$$w0rd
```

```
hostname#
```

次に、レベル 10 の特権 EXEC モードを開始する例を示します。

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

関連コマンド

コマンド	説明
enable password	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。

enable（webvpn）

以前に設定したインターフェイスで WebVPN または電子メール プロキシ アクセスをイネーブルにするには、enable コマンドを使用します。WebVPN の場合は、webvpn モードでこのコマンドを使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）については、該当する電子メール プロキシ モードでこのコマンドを使用します。インターフェイスで WebVPN をディセーブルにするには、このコマンドの **no** バージョンを使用します。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、Outside という名前のインターフェイスで WebVPN をイネーブルにする方法の例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable Outside
```

次に、Outside という名前のインターフェイスで POP3S 電子メール プロキシを設定する方法の例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# enable Outside
```

enable gprs

RADIUS アカウンティングで GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスします。セキュリティ アプライアンスは、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージ内に 3GPP VSA 26-10415 があるかどうかをチェックします。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable gprs

no enable gprs

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
radius アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このオプションは、デフォルトで無効です。この機能をイネーブルにするには、GTP ライセンスが必要です。

例

次に、RADIUS アカウンティングで GPRS をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。15 以外のレベルのパスワードを削除するには、このコマンドの **no** 形式を使用します。レベル 15 のパスワードは削除できません。

enable password *password* **[level** *level*] [**encrypted**]

no enable password level *level*

構文の説明

encrypted	（任意）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由で別のセキュリティ アプライアンスにパスワードをコピーする必要があるが、元のパスワードを把握していない場合は、暗号化されたパスワードとこのキーワードを指定して **enable password** コマンドを入力できます。通常、**show running-config enable** コマンドを入力した場合にのみこのキーワードが表示されます。
level *level*	（任意）0 ～ 15 の特権レベルのパスワードを設定します。
password	3 ～ 32 文字の英数字および特殊文字から構成されるストリングとしてパスワードを設定します（大文字と小文字は区別されます）。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

イネーブル レベル 15（デフォルト レベル）のデフォルトのパスワードはブランクです。パスワードをブランクにリセットする場合は、*password* 引数にテキストを指定しません。

マルチ コンテキスト モードでは、システム コンフィギュレーションおよび各コンテキストに対してイネーブル パスワードを作成できます。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド認可（**aaa authorization command** コマンドを使用して **LOCAL** キーワードを指定）を設定し、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。ローカル コマンド認可を設定しない場合、イネーブル レベルは無視されて、設定したレベルにかかわらずレベル 15 へのアクセスが可能になります。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。

例

次に、イネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd
```

次に、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

次に、イネーブル パスワードを、別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定する例を示します。

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードを開始します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

endpoint

H.323 プロトコル インスペクションの HSI グループにエンドポイントを追加するには、HSI グループ コンフィギュレーション モードで **endpoint** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

構文の説明

if_name	エンドポイントがセキュリティ アプライアンスに接続するときに通過するインターフェイス。
ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントを設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HSI グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション ポリシー マップの HSI グループにエンドポイントを追加する例を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

endpoint-mapper

DCERPC インスペクションのエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

構文の説明

epm-service-only	バインディング時にエンドポイント マッパー サービスを適用することを指定します。
lookup-operation	エンドポイント マッパー サービスのルックアップ動作をイネーブルにすることを指定します。
timeout *value*	ルックアップ動作におけるピンホールのタイムアウトを指定します。範囲は、0:0:1 ～ 1193:0:0 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、DCERPC ポリシー マップにエンドポイント マッパーを設定する例を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

enforcenextupdate

CRL の NextUpdate フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。期限が切れた NextUpdate フィールドがある場合や、NextUpdate フィールドがない場合を許容するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は強制（オン）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ca-crl コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドが設定されている場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。このコマンドが使用されていない場合、セキュリティ アプライアンスでは、CRL に NextUpdate フィールドがない場合や、期限が切れた NextUpdate フィールドがある場合が許容されます。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central に対して、期限が切れていない NextUpdate フィールドが CRL に存在することを必須とする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数（24）にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** の時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合（登録しようとしてダウンロードに失敗した場合など）、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

（注） この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

enrollment retry count

再試行回数を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。証明書を要求した後、セキュリティ アプライアンスは CA からの証明書の受信を待ちます。セキュリティ アプライアンスは、設定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。セキュリティ アプライアンスは、応答を受信するか、または設定されている再試行間隔が終了するまで、要求を繰り返し送信します。デフォルトの再試行回数設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count

構文の説明

number	登録要求の送信を試行する最大回数。有効な範囲は、0、および 1 ～ 100 回の再試行です。

デフォルト

number のデフォルト設定は 0（無制限）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行回数を 20 回に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。

enrollment retry period

再試行間隔を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。証明書を要求した後、セキュリティ アプライアンスは CA からの証明書の受信を待ちます。セキュリティ アプライアンスは、指定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。デフォルトの再試行間隔設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period

構文の説明

minutes	登録要求の送信を試行する間隔（分単位）。有効な範囲は、1 ～ 60 分です。

デフォルト

デフォルトの設定は 1 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行間隔を 10 分に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	すべての登録パラメータを、システムのデフォルト値に戻します。
enrollment retry count	登録要求の再試行回数を定義します。

enrollment terminal

このトラストポイントでカット アンド ペースト登録（手動登録とも呼ばれます）を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment terminal

no enrollment terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の CA 登録にカット アンド ペースト方式を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment url	このトラストポイントに対して自動登録（SCEP）を指定して、URL を設定します。

enrollment url

このトラストポイントの登録に自動登録（SCEP）を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url

構文の説明

url	自動登録の URL の名前を指定します。最大の長さは 1000 文字です（実質的に無制限です）。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に URL https://enrollsite における SCEP 登録を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数（24）にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** の時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合（登録しようとしてダウンロードに失敗した場合など）、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

（注） この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

eou allow

NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで **eou allow** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

eou allow {audit | clientless | none}

no eou allow {audit | clientless | none}

構文の説明

audit	監査サーバでクライアントレス認証を実行します。
clientless	Cisco ACS でクライアントレス認証を実行します。
none	クライアントレス認証をディセーブルにします。

デフォルト

デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	audit オプションを追加しました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、次の両方の条件が満たされている場合にのみこのコマンドが使用されます。

- NAC ポリシー タイプとして NAC フレームワークを使用するようにグループ ポリシーが設定されていること。
- セッションのホストが EAPoUDP 要求に応答しないこと。

例

次に、ACS を使用したクライアントレス認証の実行をイネーブルにする例を示します。

```
hostname(config)# eou allow clientless
hostname(config)#
```

次に、監査サーバを使用してクライアントレス認証を実行するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# eou allow audit
hostname(config)#
```

次に、監査サーバの使用をディセーブルにする例を示します。

```
hostname(config)# no eou allow clientless
hostname(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou clientless	NAC フレームワーク コンフィギュレーションのクライアントレス認証で ACS に対して送信されるユーザ名およびパスワードを変更します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou clientless

NAC フレームワーク コンフィギュレーションにおけるクライアントレス認証でアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

構文の説明

password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するパスワードを変更する場合に入力します。
password	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。
username	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するユーザ名を変更する場合に入力します。
username	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているユーザ名を入力します。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。

デフォルト

username 属性と password 属性のデフォルト値は、両方とも clientless です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、クライアントレス認証のユーザ名を sherlock に変更する例を示します。

```
hostname(config)# eou clientless username sherlock
hostname(config)#
```

次に、クライアントレス認証のユーザ名をデフォルト値である clientless に変更する例を示します。

```
hostname(config)# no eou clientless username
hostname(config)#
```

次に、クライアントレス認証のパスワードを secret に変更する例を示します。

```
hostname(config)# eou clientless password secret
hostname(config)#
```

次に、クライアントレス認証のパスワードをデフォルト値である clientless に変更する例を示します。

```
hostname(config)# no eou clientless password
hostname(config)#
```

関連コマンド

コマンド	説明
eou allow	NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou initialize

1 つ以上の NAC フレームワーク セッションに割り当てられているリソースをクリアして、各セッションに対して新しい無条件のポスチャ検証を開始するには、特権 EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	このセキュリティ アプライアンス上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられているアクセス ポリシー（つまりダウンロードされた ACL）が変更されたりしたときに、セッションに割り当てられているリソースをクリアする場合は、このコマンドを使用します。このコマンドを入力すると、ポスチャ検証に使用される EAPoUDP アソシエーションおよびアクセス ポリシーが消去されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize all
hostname
```

次に、tg1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize group tg1
hostname
```

次に、IP アドレス 209.165.200.225 を持つエンドポイントの NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou max-retry

セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

構文の説明

retries	再送信タイマーが期限切れになった場合に再送信する回数を制限します。値は 1 ～ 3 の範囲で入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP の再送信回数を 1 に制限する例を示します。

```
hostname(config)# eou max-retry 1
hostname(config)#
```

次に、EAP over UDP の再送信回数をデフォルト値である 3 に変更する例を示します。

```
hostname(config)# no eou max-retry
hostname(config)#
```

関連コマンド

eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou port

NAC フレームワーク コンフィギュレーションにおいて、Cisco Trust Agent との EAP over UDP 通信に使用するポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

構文の説明

port_number	EAP over UDP 通信用に指定するクライアント エンドポイントのポート番号。この番号は、Cisco Trust Agent に設定するポート番号です。値は 1024 ～ 65535 の範囲で入力します。

デフォルト

デフォルト値は 21862 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP 通信のポート番号を 62445 に変更する例を示します。

```
hostname(config)# eou port 62445
hostname(config)#
```

次に、EAP over UDP 通信のポート番号をデフォルト値に変更する例を示します。

```
hostname(config)# no eou port
hostname(config)#
```

関連コマンド

debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。

eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
show vpn-session_summary.db	VLAN マッピング セッション データを含む、IPSec、Cisco AnyConnect、NAC の各セッションの数を表示します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

eou revalidate

1 つ以上の NAC フレームワーク セッションのポスチャ再検証をただちに実行するには、特権 EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	このセキュリティ アプライアンス上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ピアのポスチャ、または割り当てられているアクセス ポリシー（つまりダウンロードされた ACL が存在する場合その ACL）が変更された場合にこのコマンドを使用します。このコマンドは、新しい無条件のポスチャ検証を開始します。コマンド入力前に有効であったポスチャ検証および割り当てられているアクセス ポリシーは、新しいポスチャ検証に成功または失敗するまでは引き続き有効となります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを再検証する例を示します。

```
hostname# eou revalidate all
hostname
```

次に、tg-1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを再検証する例を示します。

```
hostname# eou revalidate group tg-1
```

```
hostname
```

次に、IP アドレス 209.165.200.225 を持つエンドポイントの NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。

eou timeout

NAC フレームワーク コンフィギュレーションにおいて、リモート ホストに対して EAP over UDP メッセージを送信した後に待機する秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

構文の説明

hold-period	EAPoUDP 再試行回数分の EAPoUDP メッセージを送信した後に待機する最大時間。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。このタイマーが期限切れになった場合、セキュリティ アプライアンスはリモート ホストとの新しい EAP over UDP アソシエーションを開始します。
retransmit	1 回の EAPoUDP メッセージ送信後に待機する最大時間。リモート ホストから応答があると、このタイマーはクリアされます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。タイマーが期限切れになると、セキュリティ アプライアンスはリモート ホストに対して EAPoUDP メッセージを再送信します。
seconds	セキュリティ アプライアンスが待機する秒数。hold-period 属性には 60 ～ 86400 の範囲の値を、retransmit 属性には 1 ～ 60 の範囲の値を入力します。

デフォルト

hold-period 属性のデフォルト値は 180 です。

retransmit 属性のデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更する例を示します。

```
hostname(config)# eou timeout hold-period 120
```

```
hostname(config)#
```

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更する例を示します。

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

次に、再送信タイマーを 6 秒に変更する例を示します。

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

次に、再送信タイマーをデフォルト値に変更する例を示します。

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou max-retry	セキュリティ アプライアンスがリモート コンピュータに対して EAP over UDP メッセージを再送信する回数を変更します。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで **erase** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きしてファイル システムを消去し、ファイル システムを再インストールします。

erase [**disk0: | disk1: | flash:**]

構文の説明

disk0*:*	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部コンパクト フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。 **注意** フラッシュ メモリを消去すると、フラッシュ メモリ内に保管されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保管してください。 ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上の全データを消去し、デバイスの空のファイル システム割り当てテーブルを再書き込みします。

（非表示のシステム ファイルを除く）表示されているすべてのファイルを削除する場合は、**erase** コマンドではなく **delete /recursive** コマンドを入力します。

（注）　Cisco PIX セキュリティ アプライアンスでは、**erase** コマンドおよび **format** コマンドは両方とも、0xFF パターンを使用してユーザ データを破棄します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次に、ファイル システムを消去して再フォーマットする例を示します。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く表示されているすべてのファイルを削除します。
format	（非表示のシステム ファイルを含む）すべてのファイルを消去して、ファイル システムをフォーマットします。

esp

IPSec パススルー インスペクションで esp トンネルおよび AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

構文の説明

esp	esp トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *num*	1 つのクライアントからの最大トンネル数を指定します。
timeout *time*	esp トンネルのアイドル タイムアウトを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、UDP 500 のトラフィックを許可する例を示します。

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

established

確立された接続に基づく、ポートへの戻り接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

構文の説明

est_protocol	確立された接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dest_port	確立された接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（任意）指定したポートから発信される戻りプロトコル接続を許可します。
permitto	（任意）指定したポートに着信する戻りプロトコル接続を許可します。
port [*-port*]	（任意）戻り接続の（UDP または TCP）宛先ポートを指定します。
protocol	（任意）戻り接続で使用される IP プロトコル（UDP または TCP）。
source_port	（任意）確立された接続のルックアップに使用する送信元ポートを指定します

デフォルト

デフォルトの設定は次のとおりです。

- *dest_port*：0（ワイルドカード）
- *source_port*：0（ワイルドカード）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **to** および **from** が CLI から削除されました。代わりにキーワード **permitto** および **permitfrom** を使用します。

使用上のガイドライン

established コマンドを使用すると、セキュリティ アプライアンス経由の発信接続の戻りアクセスを許可できます。このコマンドは、ネットワークから発信され、セキュリティ アプライアンスによって保護されている元の接続、および外部ホストからの同じ 2 つのデバイス間の着信戻り接続に対して動作します。**established** コマンドでは、接続のルックアップに使用する宛先ポートを指定できます。宛先

ポートを指定することによって、コマンドをより細かく制御でき、宛先ポートは既知であるが送信元ポートは不明であるプロトコルをサポートできます。**permitto** および **permitfrom** キーワードでは、リターン インバウンド接続を定義します。

注意　**established** コマンドでは、常に **permitto** キーワードおよび **permitfrom** キーワードを指定することを推奨します。これらのキーワードを指定しないで **established** コマンドを使用すると、外部システムに接続した場合にそれらのシステムから接続に関連する内部ホストに対して無制限に接続が可能となるため、セキュリティのリスクが発生します。このような状況は、内部システムの攻撃に悪用される可能性があります。

例

次に、**established** コマンドを正しく使用しない場合にセキュリティ違反が発生する可能性があることを示すいくつかの例を示します。

次に、内部システムから外部ホストのポート 4000 に TCP 接続を確立した場合に、外部ホストから任意のプロトコルを使用して任意のポートに戻り接続を確立できることを示す例を示します。

```
hostname(config)# established tcp 4000 0
```

プロトコルで使用されるポートが規定されていない場合は、送信元ポートおよび宛先ポートに **0** を指定できます。ワイルドカード ポート（0）は、必要な場合にのみ使用します。

```
hostname(config)# established tcp 0 0
```

（注）　**established** コマンドが正しく動作するためには、クライアントは **permitto** キーワードで指定されたポートでリッスンする必要があります。

established コマンドは、**nat 0** コマンドとともに使用できます（**global** コマンドがない場合）。

（注）　**established** コマンドは、PAT とともに使用することはできません。

セキュリティ アプライアンスでは、**established** コマンドを利用することによって XDMCP がサポートされます。

注意　セキュリティ アプライアンスを通して XWindows システム アプリケーションを使用すると、セキュリティのリスクが発生する可能性があります。

デフォルトで、XDMCP はオンになっていますが、次のように **established** コマンドを入力しないとセッションが完了しません。

```
hostname(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP 実装ホスト（UNIX または Reflection X）から外部の XDMCP 実装 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP によって TCP ベースの XWindows セッションがネゴシエートされ、後続の TCP 戻り接続が許可されます。リターン トラフィックの送信元ポートは不明であるため、*source_port* フィールドには 0（ワイルドカード）を指定します。*dest_port* は 6000 + *n* となります。*n* は、ローカルのディスプレイ番号を表します。この値を変更するには、次の UNIX コマンドを使用します。

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

（ユーザ対話に基づいて）数多くの TCP 接続が生成され、これらの接続の送信元ポートが不明であるため、**established** コマンドが必要となります。宛先ポートのみがスタティックです。セキュリティ アプライアンスでは、XDMCP フィックスアップが透過的に実行されます。コンフィギュレーションは必要ありませんが、TCP セッションを確立できるように **established** コマンドを入力する必要があります。

次に、プロトコル A、宛先ポート B、送信元ポート C を使用した 2 つのホスト間の接続の例を示します。セキュリティ アプライアンス経由でプロトコル D（プロトコル D はプロトコル A とは異なっていてもかまいません）による戻り接続を許可するには、送信元ポートがポート F に、宛先ポートがポート E に対応している必要があります。

```
hostname(config)# established A B C permitto D E permitfrom D F
```

次に、TCP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。セキュリティ アプライアンスでは、TCP 宛先ポート 6061 および任意の TCP 送信元ポートを使用したホスト間のリターン トラフィックが許可されます。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

次に、UDP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。セキュリティ アプライアンスでは、TCP 宛先ポート 6061 および TCP 送信元ポート 1024 ～ 65535 を使用したホスト間のリターン トラフィックが許可されます。

```
hostname(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

次に、ローカル ホストから外部ホストにポート 9999 への TCP 接続を開始する例を示します。この例では、外部ホストのポート 4242 からローカル ホストのポート 5454 へのパケットが許可されます。

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

exceed-mss

スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

構文の説明

allow	MSS を超えるパケットを許可します。この設定は、デフォルトです。
drop	MSS を超えるパケットをドロップします。

デフォルト

パケットは、デフォルトで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)/8.0(4)	デフォルトが **drop** から **allow** に変更されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。

例

次に、MSS を超えた場合にポート 21 のフローをドロップする例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss drop
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection advanced-options	TCP 正規化を含む、高度な接続機能を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

exempt-list

ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **exempt-list** コマンドを使用します。免除リストからエントリを削除するには、このコマンドの **no** 形式を使用して、削除するエントリのオペレーティング システムおよび ACL を指定します。

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

構文の説明

acl-name	セキュリティ アプライアンス コンフィギュレーションに存在する ACL の名前。指定する場合は、**filter** キーワードの後に指定する必要があります。
disable	次の 2 つの機能のいずれかを実行します。 • "os-name" の後に入力した場合、セキュリティ アプライアンスは、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 • *acl-name* の後に入力した場合、セキュリティ アプライアンスは指定したオペレーティング システムを免除しますが、関連するトラフィックに ACL を割り当てません。
filter	コンピュータのオペレーティング システムが *os name* に一致する場合にトラフィックをフィルタリングするための ACL を適用します。**filter** と *acl-name* のペアは省略可能です。
os	オペレーティング システムをポスチャ検証から免除します。
os name	オペレーティング システム名。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば `"Windows XP"`）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名が **vpn-nac-exempt** から **exempt-list** に変更されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドでオペレーティング システムを指定しても、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

no exempt-list コマンドを入力すると、NAC フレームワーク ポリシーからすべての免除が削除されます。エントリを指定してこのコマンドの **no** 形式を発行すると、そのエントリが免除リストから削除されます。

NAC ポリシーに関連付けられている免除リストからすべてのエントリを削除するには、キーワードを指定しないでこのコマンドの **no** 形式を使用します。

例

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
hostname(config-group-policy)# exempt-list os "Windows XP"
hostname(config-group-policy)
```

次に、Windows XP を実行するすべてのホストを免除して、これらのホストのトラフィックに ACL acl-1 を適用する例を示します。

```
hostname(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

次に、免除リストから上記の例と同じエントリを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no exempt-list
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
show vpn-session_summary.db	IPSec、Cisco AnyConnect、および NAC の各セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了して、セッションからログアウトする方法の例を示します。

```
hostname(config)# exit
hostname# exit

Logoff
```

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
hostname(config)# exit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了するか、または特権 EXEC モードやユーザ EXEC モードからログアウトします。

expiry-time

再検証しないでオブジェクトをキャッシュする有効期限を設定するには、キャッシュ コンフィギュレーション モードで **expiry-time** コマンドを使用します。コンフィギュレーションから有効期限を削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

expiry-time *time*

no expiry-time

構文の説明

time	セキュリティ アプライアンスが再検証しないでオブジェクトをキャッシュする時間（分）。

デフォルト

1 分。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

有効期限とは、セキュリティ アプライアンスが再検証しないでオブジェクトをキャッシュする時間（分）を指します。再検証では、内容が再度チェックされます。

例

次に、有効期限を 13 分に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。

コマンド	説明
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

export

証明書をクライアントにエクスポートすることを指定するには、CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

構文の説明

certificate *trustpoint_name*　クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL プロバイダー コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用して、証明書をクライアントにエクスポートすることを指定します。トラストポイント名は、**crypto ca trustpoint** コマンドで定義します。証明書は、CTL クライアントで構成された証明書信頼リスト ファイルに追加されます。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。

コマンド	説明
client	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

export webvpn customization

クライアントレス SSL VPN ユーザに表示される画面をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn customization** コマンドを使用します。

export webvpn customization *name url*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大 64 文字です。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、クライアントレス SSL VPN ユーザに表示される画面（ログイン画面、ログアウト画面、ポータル ページ、使用可能な言語など）をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度セキュリティ アプライアンスにインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

export webvpn customization コマンドを使用してカスタマイゼーション オブジェクトをエクスポートし、XML タグを変更し、**import webvpn customization** コマンドを使用して新しいオブジェクトとしてファイルをインポートできます。

例

次に、デフォルトのカスタマイゼーション オブジェクト（DfltCustomization）をエクスポートして、dflt_custom という名前の XML ファイルを作成する例を示します。

```
hostname# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
```

```
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
hostname#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn translation-table

SSL VPN 接続を確立するリモート ユーザに表示される用語を変換するために使用される変換テーブルをエクスポートするには、特権 EXEC モードで **export webvpn translation-table** コマンドを使用します。

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

構文の説明

language	事前にインポート済みの変換テーブル名を指定します。値は、ブラウザの言語オプションの表現に従って入力します。
translation_domain	機能エリアおよび関連するメッセージです。使用上のガイドラインのセクションに、使用可能な変換ドメインがリストされています。
url	オブジェクトの URL を指定します。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

リモート ユーザに表示される各機能エリアとそのメッセージには独自の変換ドメインがあります。この変換ドメインは *translation_domain* 引数で指定します。次の表に、変換ドメインおよび、変換される機能領域を示します。

表 12-1　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。

変換ドメイン	変換される機能エリア
banners	リモート ユーザに表示されるバナーと、VPN アクセスが拒否されたときのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。

変換テンプレートは変換テーブルと同じ形式の XML ファイルですが、変換内容はすべて空です。セキュリティ アプライアンスのソフトウェア イメージ パッケージには、標準機能の一部として各ドメイン用のテンプレートが含まれています。プラグインのテンプレートはプラグインに付属しており、独自の変換ドメインを定義します。クライアントレス ユーザのログインおよびログアウト ページ、ポータル ページ、および URL ブックマークはカスタマイズが可能なため、セキュリティ アプライアンスは **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

以前にインポートされた変換テーブルをエクスポートすると、URL の場所にそのテーブルの XML ファイルが作成されます。**show import webvpn translation-table** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

export webvpn translation-table コマンドを使用してテンプレートまたは変換テーブルをダウンロードし、メッセージを変更し、**import webvpn translation-table** コマンドを使用して変換テーブルをインポートします。

例

次に、変換ドメイン *customization* 用のテンプレートをエクスポートする例を示します。このドメインは、クライアントレス SSL VPN 接続を確立するリモート ユーザがカスタマイズおよび表示可能なログイン ページ、ログアウト ページ、ポータル ページ、およびすべてのメッセージを変換するために使用します。セキュリティ アプライアンスは、*Sales* という名前の XML ファイルを作成します。

```
hostname# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、*zh* という名前の、以前にインポートされた中国語用変換テーブルをエクスポートする例を示します。この短縮形 zh は、Microsoft Internet Explorer ブラウザの [Internet Options] で中国語に指定されている短縮形に準拠しています。セキュリティ アプライアンスは、*Chinese* という名前の XML ファイルを作成します。

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

export webvpn url-list

URL リストをリモートの場所にエクスポートするには、特権 EXEC モードで **export webvpn url-list** コマンドを使用します。

export webvpn url-list *name url*

構文の説明

name	URL リストを識別する名前。最大 64 文字です。
URL	URL リストのソースへのリモート パス。最大 255 文字です。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

WebVPN には、デフォルトで URL リストはありません。

export webvpn url-list コマンドを使用して、Template というオブジェクトをダウンロードできます。Template は、変更または削除できません。Template の内容を編集してカスタム URL リストとして保存し、**import webvpn url-list** コマンドを使用してインポートし、カスタム URL リストを追加できます。

インポート済みの URL リストをエクスポートすると、URL の場所にそのリストの XML ファイルが作成されます。**show import webvpn url-list** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

例

次に、URL リスト *servers* をエクスポートする例を示します。

```
hostname# export webvpn url-list servers2 tftp://209.165.200.225
hostname#
```

関連コマンド

コマンド	説明
import webvpn url-list	URL リストをインポートします。

revert webvpn url-list	キャッシュ メモリから URL リストを削除します。
show import webvpn url-list	インポート済みの URL リストに関する情報を表示します。

export webvpn webcontent

リモートのクライアントレス SSL VPN ユーザに表示される、フラッシュ メモリ内のインポート済みコンテンツをエクスポートするには、特権 EXEC モードで **export webvpn webcontent** コマンドを使用します。

export webvpn webcontent <*source url*> <*destination url*>

構文の説明

<*source url*>	コンテンツがあるセキュリティ アプライアンスのフラッシュ メモリの URL。最大 64 文字です。
<*destination url*>	エクスポート先の URL。最大 255 文字です。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

webcontent オプションを使用してエクスポートされるコンテンツは、リモートのクライアントレス ユーザに表示されるコンテンツです。これには、クライアントレス ポータルに表示されるインポート済みのヘルプ コンテンツや、カスタマイゼーション オブジェクトによって使用されるロゴなどがあります。

export webvpn webcontent コマンドの後に疑問符（**?**）を入力すると、エクスポート可能なコンテンツのリストを表示できます。次に例を示します。

```
hostname# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

例

次に、tftp を使用してファイル *logo.gif* を、*logo_copy.gif* というファイル名で 209.165.200.225 にエクスポートする例を示します。

```
hostname# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

関連コマンド

コマンド	説明
import webvpn webcontent	クライアントレス SSL VPN ユーザに表示されるコンテンツをインポートします。
revert webvpn webcontent	コンテンツをフラッシュ メモリから削除します。
show import webvpn webcontent	インポートされたコンテンツに関する情報を表示します。

failover

フェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover** コマンドを使用します。フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover

no failover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバーはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーションでのフェールオーバーのイネーブルまたはディセーブルに限定されました（**failover active** コマンドを参照）。

使用上のガイドライン

フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

ASA 5505 デバイスでは、ステートレス フェールオーバーのみが、Easy VPN ハードウェア クライアントとして動作していないときにのみ許可されます。

例

次に、フェールオーバーをディセーブルにする例を示します。

```
hostname(config)# no failover
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover active

スタンバイのセキュリティ アプライアンスまたはフェールオーバー グループをアクティブ ステートに切り替えるには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブなセキュリティ アプライアンスまたはフェールオーバー グループをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

構文の説明

group *group_id*	（任意）アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、フェールオーバー グループを含むように変更されました。

使用上のガイドライン

スタンバイ ユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブ ユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合は、すべてのアクティブな接続がドロップされるため、フェールオーバー実行後にクライアントは接続を再確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ使用できます。Active/Active フェールオーバー ユニットでフェールオーバー グループを指定しないで **failover active** コマンドを入力すると、ユニットのすべてのグループがアクティブになります。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
hostname# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	セキュリティ アプライアンスを障害発生状態からスタンバイに移行します。

failover exec

フェールオーバー ペアの特定のユニットに対してコマンドを実行するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **failover exec** コマンドを使用します。

failover exec {**active** | **standby** | **mate**} *cmd_string*

構文の説明

active	コマンドをフェールオーバー ペアのアクティブ ユニットまたはフェールオーバー グループに対して実行することを指定します。アクティブ ユニットまたはフェールオーバー グループに対して入力されたコンフィギュレーション コマンドは、スタンバイ ユニットまたはフェールオーバー グループに複製されます。
cmd_string	実行するコマンド。show コマンド、コンフィギュレーション コマンド、および EXEC コマンドがサポートされています。
mate	コマンドをフェールオーバー ピアに対して実行することを指定します。
standby	コマンドをフェールオーバー ペアのスタンバイ ユニットまたはフェールオーバー グループに対して実行することを指定します。スタンバイ ユニットまたはフェールオーバー グループに対して実行されたコンフィギュレーション コマンドは、アクティブ ユニットまたはフェールオーバー グループには複製されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

failover exec コマンドを使用して、フェールオーバー ペアの特定のユニットに対してコマンドを送信できます。

コンフィギュレーション コマンドはアクティブ ユニットまたはコンテキストからスタンバイ ユニットまたはコンテキストに複製されるため、いずれのユニットにログインしているかにかかわらず、**failover exec** コマンドを使用して正しいユニットにコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ ユニットにログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ ユニットに送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置またはコンテキストへのコンフィギュレーション コマンドの送信には、**failover exec** コマンドを使用しないでください。これらのコンフィギュレーションの変更はアクティブ装置に複製されないため、2 つのコンフィギュレーションが同期されなくなります。

コンフィギュレーション、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されます。したがって、**failover exec** コマンドを使用して、ピア装置で **show** コマンドを発行し、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

コマンド モード

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトで、**failover exec** のコマンド モードは、指定したデバイスに対するグローバル コンフィギュレーション モードです。このコマンド モードを変更するには、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。

指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。たとえば、フェールオーバー ペアのアクティブ ユニットにログインしており、グローバル コンフィギュレーション モードで次のコマンドを発行した場合、セッションのコマンド モードはグローバル コンフィギュレーション モードのままですが、**failover exec** コマンドを使用して送信されるすべてのコマンドはインターフェイス コンフィギュレーション モードで実行されます。

```
hostname(config)# failover exec interface GigabitEthernet0/1
hostname(config)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ ユニットでインターフェイス コンフィギュレーション モードであるときに、**failover exec** のコマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。

```
hostname(config-if)# failover exec active router ospf 100
hostname(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

セキュリティに関する注意事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防止するには、**failover key** コマンドを使用してフェールオーバー リンクを暗号化する必要があります。

制限事項

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしているユニットでそのコンテキストに変更する必要があります。
- 次のコマンドと **failover exec** コマンドを一緒に使用することはできません。
  - **changeto**
  - **debug**（**undebug**）
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。

- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーション コマンドを入力した場合、現在の装置でグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** *コマンド*のような、再帰的な failover exec コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

例

次に、**failover exec** コマンドを使用して、アクティブ ユニットのフェールオーバー情報を表示する例を示します。コマンドはアクティブ ユニットで実行されるため、コマンドはローカルで実行されます。

```
hostname(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
hostname(config)#
```

次に、**failover exec** コマンドを使用して、ピア ユニットのフェールオーバー ステータスを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
hostname(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

次に、**failover exec** コマンドを使用して、フェールオーバー ピアのフェールオーバー コンフィギュレーションを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
hostname(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、スタンバイ ユニットからアクティブ ユニットにコンテキストを作成する例を示します。コマンドは、アクティブ ユニットからスタンバイ ユニットに複製されます。「Creating context」というメッセージが 2 回表示されていることに注意してください。1 回めは、コンテキスト作成時に **failover exec** コマンドによってピア ユニットから出力されたものであり、2 回めは複製されたコマンドによってローカルにコンテキストが作成されたときにローカル ユニットから出力されたものです。

```
hostname(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

hostname(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

hostname(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

次に、**failover exec** コマンドを使用してスタンバイ ステートのフェールオーバー ピアにコンフィギュレーション コマンドを送信したときに警告が返され、その警告が表示される例を示します。

```
hostname# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

       **** WARNING ****
       Configuration Replication is NOT performed from Standby unit to Active unit.
       Configurations are no longer synchronized.
hostname(config)#
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイ ユニットに送信する例を示します。

```
hostname(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
```

```
        284 packets output, 26976 bytes
        0 packets dropped
        1 minute input rate 0 pkts/sec,  21 bytes/sec
        1 minute output rate 0 pkts/sec,  23 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 0 pkts/sec,  21 bytes/sec
        5 minute output rate 0 pkts/sec,  24 bytes/sec
        5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
        MAC address 000b.fcf8.c291, MTU 1500
        IP address 192.168.0.11, subnet mask 255.255.255.0
        214 packets input, 26902 bytes, 0 no buffer
        Received 1 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        215 packets output, 27028 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
        214 packets input, 23050 bytes
        215 packets output, 23140 bytes
        0 packets dropped
        1 minute input rate 0 pkts/sec,  21 bytes/sec
        1 minute output rate 0 pkts/sec,  21 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 0 pkts/sec,  21 bytes/sec
        5 minute output rate 0 pkts/sec,  21 bytes/sec
        5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c293, MTU 1500
        IP address 10.0.5.2, subnet mask 255.255.255.0
        1991 packets input, 408734 bytes, 0 no buffer
        Received 1 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        1835 packets output, 254114 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
        1913 packets input, 345310 bytes
        1755 packets output, 212452 bytes
        0 packets dropped
        1 minute input rate 1 pkts/sec,  319 bytes/sec
        1 minute output rate 1 pkts/sec,  194 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 1 pkts/sec,  318 bytes/sec
        5 minute output rate 1 pkts/sec,  192 bytes/sec
        5 minute drop rate, 0 pkts/sec
.
.
.
```

次に、ピア ユニットに対して不正なコマンドを発行したときにエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
hostname# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーがディセーブルの場合に **failover exec** コマンドを使用してエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
hostname(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー関連のデバッグ メッセージを表示します。
debug xml	**failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。
show failover exec	**failover exec** のコマンド モードを表示します。

failover group

Active/Active フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで **failover group** コマンドを使用します。フェールオーバー グループを削除するには、このコマンドの **no** 形式を使用します。

failover group *num*

no failover group *num*

構文の説明

num	フェールオーバー グループの番号。有効な値は、1 または 2 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モードが設定されたデバイスのシステム コンテキストにのみ追加できます。フェールオーバー グループは、フェールオーバーがディセーブルになっているときに限り作成および削除できます。

このコマンドを入力すると、フェールオーバー グループ コマンド モードが開始されます。フェールオーバー グループ コンフィギュレーション モードでは、**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドを使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

（注）　**failover polltime interface**、**failover interface-policy**、**failover replication http**、および **failover mac address** コマンドは、Active/Active フェールオーバー コンフィギュレーションでは効果がありません。これらは、**polltime interface**、**interface-policy**、**replication http**、および **mac address** の各フェールオーバー グループ コンフィギュレーション モード コマンドによって上書きされます。

フェールオーバー グループを削除するときは、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないすべてのコンテキストは、デフォルトでフェールオーバー グループ 1 に割り当てられます。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

（注）　同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上に重複した MAC アドレスが存在しないようにするには、**mac address** コマンドを使用して、各物理インターフェイスに対して仮想アクティブ MAC アドレスおよび仮想スタンバイ MAC アドレスを割り当てる必要があります。

例

次に、2 つのフェールオーバー グループのコンフィギュレーションの例（抜粋）を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
asr-group	非対称ルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
mac address	フェールオーバー グループ内のコンテキストに対して仮想 MAC アドレスを定義します。
polltime interface	モニタ対象インターフェイスに送信される hello メッセージ間の時間を指定します。
preempt	高いプライオリティを持つユニットが、リブート後にアクティブ ユニットとなることを指定します。
primary	フェールオーバー グループにおいて、プライマリ ユニットに対してより高いプライオリティを指定します。
replication http	選択したフェールオーバー グループに対して、HTTP セッションのレプリケーションを指定します。
secondary	フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを指定します。

failover interface ip

フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスに対して IP アドレスおよびマスクを指定するには、グローバル コンフィギュレーション モードで **failover interface ip** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover interface ip *if_name ip_address mask* **standby** *ip_address*

no failover interface ip *if_name ip_address mask* **standby** *ip_address*

構文の説明

if_name	フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスのインターフェイス名。
ip_address mask	プライマリ モジュールのフェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスに対して IP アドレスおよびマスクを指定します。
standby *ip_address*	セカンダリ モジュールがプライマリ モジュールと通信する場合に使用する IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスは、セキュリティ アプライアンスがトランスペアレント ファイアウォール モードで動作している場合でもレイヤ 3 の機能であり、システムに対してグローバルです。

マルチ コンテキスト モードでは、システム コンテキストにフェールオーバーを設定します（**monitor-interface** コマンドを除く）。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、フェールオーバー インターフェイスの IP アドレスおよびマスクを指定する例を示します。

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定したインターフェイスの状態をモニタします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover interface-policy

モニタリングによってインターフェイスの障害が検出された場合のフェールオーバーのポリシーを指定するには、グローバル コンフィギュレーション モードで **failover interface-policy** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

構文の説明

num	パーセンテージとして使用される場合は 1 ～ 100 の数値を、数値として使用される場合は 1 ～インターフェイスの最大数を指定します。
%	（任意）*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *num* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が設定されているポリシーの基準を満たし、他方のセキュリティ アプライアンスが正しく機能している場合、セキュリティ アプライアンスは自身を障害発生状態とマークして、フェールオーバーが行われる可能性があります（アクティブなセキュリティ アプライアンスで障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次に、2 通りの方法でフェールオーバー ポリシーを指定する例を示します。

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	ユニットおよびインターフェイスのポーリング タイムを指定します。
failover reset	障害が発生したユニットを障害が発生していない状態に復元します。
monitor-interface	フェールオーバーのためにモニタ対象にするインターフェイスを指定します。
show failover	装置のフェールオーバー状態についての情報を表示します。

failover key

フェールオーバー ペアのユニット間での暗号化および認証された通信用のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

failover key {*secret* | **hex** *key*}

no failover key

構文の説明

hex *key*	暗号キーの 16 進数値を指定します。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。
secret	英数字の共有秘密を指定します。秘密に使用できる文字数は、1 ～ 63 文字です。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover lan key** から **failover key** に変更されました。
7.0(4)	このコマンドが、**hex** *key* キーワードおよび引数を含むように変更されました。

使用上のガイドライン

ユニット間のフェールオーバー通信を暗号化および認証するには、両方のユニットに共有秘密または 16 進キーを設定する必要があります。フェールオーバー キーを指定しない場合、フェールオーバー通信はクリア テキストで送信されます。

（注） PIX セキュリティ アプライアンス プラットフォームでは、ユニットへの接続に専用のシリアル フェールオーバー ケーブルを使用している場合、フェールオーバー キーを設定しても、フェールオーバー リンク上の通信は暗号化されません。フェールオーバー キーでは、LAN ベースのフェールオーバー通信のみが暗号化されます。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、フェールオーバー ペアのユニット間でフェールオーバー通信をセキュリティ保護するための共有秘密を指定する例を示します。

```
hostname(config)# failover key abcdefg
```

次に、フェールオーバー ペアの 2 つのユニット間でフェールオーバー通信をセキュリティ保護するための 16 進キーを指定する例を示します。

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内の failover コマンドを表示します。

failover lan enable

PIX セキュリティ アプライアンスで LAN ベースのフェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover lan enable** コマンドを使用します。LAN ベースのフェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover lan enable

no failover lan enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

イネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの **no** 形式を使用して LAN ベースのフェールオーバーがディセーブルになっている場合、フェールオーバー ケーブルが接続されていると、ケーブルベースのフェールオーバーが使用されます。このコマンドは、PIX セキュリティ アプライアンスでのみ使用できます。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、LAN ベースのフェールオーバーをイネーブルにする例を示します。

```
hostname(config)# failover lan enable
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover lan interface** コマンドを使用します。フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover lan interface *if_name* {*phy_if*[*.sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[*.sub_if*] | *vlan_if*]}]

構文の説明

if_name	フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	物理インターフェイスを指定します。
sub_if	（任意）サブインターフェイス番号を指定します。
vlan_if	ASA 5505 セキュリティ アプライアンスで、VLAN インターフェイスをフェールオーバー リンクとして指定するために使用されます。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、*phy_if* 引数を含めるように変更されました。
7.2(1)	このコマンドが、*vlan_if* 引数を含むように変更されました。

使用上のガイドライン

LAN フェールオーバーでは、フェールオーバー トラフィックを送受信するための専用のインターフェイスが必要です。ただし、LAN フェールオーバー インターフェイスをステートフル フェールオーバー リンクに使用することもできます。

（注） LAN フェールオーバーとステートフル フェールオーバーの両方で同じインターフェイスを使用する場合は、LAN ベースのフェールオーバーとステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量がインターフェイスに必要です。

デバイス上の任意の未使用のイーサネット インターフェイスをフェールオーバー インターフェイスとして使用できます。現在名前が設定されているインターフェイスは指定できません。フェールオーバー インターフェイスは、通常のネットワーキング インターフェイスとしては設定されず、フェールオー

バー通信専用となります。このインターフェイスは、フェールオーバー リンク専用である必要があります（ただしステート リンクとしても使用可能）。LAN ベースのフェールオーバー リンクは、リンクにホストまたはルータのない専用スイッチを使用するか、装置を直接リンクするためのクロスオーバー イーサネット ケーブルを使用して接続できます。

（注） VLAN を使用する場合は、フェールオーバー リンク専用の VLAN を使用します。フェールオーバー リンクの VLAN を他の VLAN と共有すると、断続的にトラフィックの問題が発生したり、ping や ARP の障害が発生したりすることがあります。フェールオーバー リンクの接続にスイッチを使用する場合は、スイッチおよびセキュリティ アプライアンスでフェールオーバー リンク専用のインターフェイスを使用します。インターフェイスを、通常のネットワーク トラフィックを伝送するサブインターフェイスと共有しないでください。

マルチ コンテキスト モードで動作するシステムでは、フェールオーバー リンクはシステム コンテキストにあります。システム コンテキストに設定できるインターフェイスは、このインターフェイス、および使用されている場合はステート リンクのみです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注） フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

このコマンドの **no** 形式を使用すると、フェールオーバー インターフェイスの IP アドレス コンフィギュレーションもクリアされます。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、PIX 500 シリーズセキュリティ アプライアンスでフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink Ethernet4
```

次に、ASA 5500 シリーズセキュリティ アプライアンス（ASA 5505 セキュリティ アプライアンスを除く）でサブインターフェイスを使用してフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

次に、ASA 5505 セキュリティ アプライアンスでフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink Vlan6
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

LAN フェールオーバー設定でセキュリティ アプライアンスをプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

構文の説明

primary	セキュリティ アプライアンスをプライマリ ユニットとして指定します。
secondary	セキュリティ アプライアンスをセカンダリ ユニットとして指定します。

デフォルト

セカンダリ

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Active/Standby フェールオーバーでは、フェールオーバー ユニットに対するプライマリとセカンダリの指定によって、起動時にどのユニットがアクティブになるかが決まります。次の場合に、起動時にプライマリ ユニットがアクティブ ユニットになります。

- 最初のフェールオーバー ポーリング チェックの間に、プライマリ ユニットとセカンダリ ユニットの両方がブート シーケンスを完了している。
- プライマリ ユニットがセカンダリ ユニットよりも前に起動している。

プライマリ ユニットの起動時にすでにセカンダリ ユニットがアクティブになっている場合、プライマリ ユニットはアクティブにはならずに、スタンバイ ユニットとなります。この場合、プライマリ ユニットを強制的にアクティブ ステータスに戻すには、セカンダリ（アクティブ）ユニットで **no failover active** コマンドを発行する必要があります。

Active/Active フェールオーバーでは、各フェールオーバー グループにプライマリまたはセカンダリのユニット プリファレンスが割り当てられます。このプリファレンスによって、両方のユニットが（フェールオーバー ポーリング期間内に）同時に起動されたときに、起動時にフェールオーバー ペアのどのユニットでフェールオーバー グループのコンテキストがアクティブになるかが決まります。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、セキュリティ アプライアンスを LAN ベースのフェールオーバーのプライマリ ユニットとして設定する例を示します。

```
hostname(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover link** コマンドを使用します。ステートフル フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover link *if_name* [*phy_if*]

no failover link

構文の説明

if_name	ステートフル フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	（任意）物理インターフェイス ポートまたは論理インターフェイス ポートを指定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられているインターフェイスを共有しているか、または標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、*phy_if* 引数を含めるように変更されました。
7.0(4)	このコマンドが、標準ファイアウォール インターフェイスを受け入れるように変更されました。

使用上のガイドライン

このコマンドは、ステートフル フェールオーバーをサポートしない ASA 5505 シリーズセキュリティ アプライアンスでは使用できません。

物理または論理インターフェイス引数は、フェールオーバー通信または標準ファイアウォール インターフェイスを共有していない場合に必要となります。

failover link コマンドによって、ステートフル フェールオーバーがイネーブルになります。ステートフル フェールオーバーをディセーブルにするには、**no failover link** コマンドを入力します。専用のステートフル フェールオーバー インターフェイスを使用している場合は、**no failover link** コマンドによって、ステートフル フェールオーバー インターフェイスの IP アドレス コンフィギュレーションもクリアされます。

ステートフル フェールオーバーを使用するには、すべての状態情報を送信するためのステートフル フェールオーバー リンクを設定する必要があります。ステートフル フェールオーバー リンクを設定する方法としては、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンクに、専用のイーサネット インターフェイスを使用できます。
- LAN ベースのフェールオーバーを使用する場合は、フェールオーバー リンクを共有できます。
- 内部インターフェイスなど、通常のデータ インターフェイスを共有できます。しかし、このオプションはお勧めしません。

ステートフル フェールオーバー リンクに専用のイーサネット インターフェイスを使用する場合は、スイッチまたはクロス ケーブルを使用して、ユニットを直接接続できます。スイッチを使用する場合は、このリンク上に他のホストやルータを配置しないようにする必要があります。

（注） セキュリティ アプライアンスに直接接続されている Cisco スイッチ ポートの PortFast オプションをイネーブルにします。

ステートフル フェールオーバー リンクとしてフェールオーバー リンクを使用する場合は、使用可能なイーサネット インターフェイスのうち最も高速なインターフェイスを使用する必要があります。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

ステートフル フェールオーバー リンクとしてデータ インターフェイスを使用する場合は、そのインターフェイスをステートフル フェールオーバー リンクとして指定したときに次の警告が表示されます。

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

データ インターフェイスとステートフル フェールオーバー インターフェイスを共有すると、リプレイ攻撃を受けやすくなる場合があります。さらに、大量のステートフル フェールオーバー トラフィックがインターフェイスで送信され、そのネットワーク セグメントでパフォーマンス上の問題が発生することがあります。

（注） データ インターフェイスは、シングル コンテキストのルーテッド モードでのみステートフル フェールオーバー インターフェイスとして使用できます。

マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキストに存在します。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注） ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは、フェールオーバー時に変更されません。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれて

います。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、専用インターフェイスをステートフル フェールオーバー インターフェイスとして指定する例を示します。この例のインターフェイスには、既存のコンフィギュレーションはありません。

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover mac address

物理インターフェイスのフェールオーバー仮想 MAC アドレスを指定するには、グローバル コンフィギュレーション モードで **failover mac address** コマンドを使用します。仮想 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

構文の説明

phy_if	MAC アドレスを設定するインターフェイスの物理名です。
active_mac	アクティブなセキュリティ アプライアンスの指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。
standby_mac	スタンバイのセキュリティ アプライアンスの指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

failover mac address コマンドを使用すると、Active/Standby フェールオーバー ペアの仮想 MAC アドレスを設定できます。仮想 MAC アドレスが定義されていない場合は、各フェールオーバー ユニットが起動したときに、それらのユニットではインターフェイスのバーンドイン MAC アドレスが使用され、それらのアドレスがフェールオーバー ピアと交換されます。プライマリ ユニットのインターフェイスの MAC アドレスが、アクティブ ユニットのインターフェイスに使用されます。

ただし、両方のユニットが同時にオンラインにならず、セカンダリ ユニットが最初に起動してアクティブになった場合、セカンダリ ユニットは、自身のインターフェイスにバーンドイン MAC アドレスを使用します。その後プライマリ ユニットがオンラインになると、セカンダリ ユニットはプライマリ ユニットから MAC アドレスを取得します。この変更によりネットワーク トラフィックが中断される可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ ユニットがプライマリ ユニットよりも前にオンラインになり、アクティブ ユニットとなった場合でも、正しい MAC アドレスが使用されるようになります。

failover lan interface コマンドでは、フェールオーバーが発生した場合に IP アドレスおよび MAC アドレスが変更されないため、LAN ベースのフェールオーバーに設定されたインターフェイスでは、**failover mac address** コマンドは不要であり、使用できません。このコマンドは、セキュリティ アプライアンスが Active/Active フェールオーバーに設定されている場合には効果がありません。

コンフィギュレーションに **failover mac address** コマンドを追加する場合は、仮想 MAC アドレスを設定し、コンフィギュレーションをフラッシュ メモリに保存して、フェールオーバー ペアをリロードすることを推奨します。アクティブな接続が存在するときに仮想 MAC アドレスを追加すると、これらの接続は停止します。また、仮想 MAC アドレス指定を有効にするには、**failover mac address** コマンドを含むコンフィギュレーション全体を、セカンダリセキュリティ アプライアンスのフラッシュ メモリに書き込む必要があります。

failover mac address がプライマリ ユニットのコンフィギュレーションに指定されている場合は、セカンダリ ユニットのブートストラップ コンフィギュレーションにも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用して、フェールオーバー グループの各インターフェイスの仮想 MAC アドレスを設定します。

例

次に、intf2 という名前のインターフェイスのアクティブ MAC アドレスおよびスタンバイ MAC アドレスを設定する例を示します。

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス、コンフィギュレーション、および統計情報を表示します。

failover polltime

フェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

構文の説明

holdtime *time*	（任意）ユニットが、フェールオーバー リンクで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 45 秒です。オプションの **msec** キーワードを使用した場合は、800 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。
poll_time	hello メッセージ間の時間。 有効な値は 1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合は、200 ～ 999 ミリ秒です。
unit	（任意）コマンドがユニットのポーリング タイムおよびホールド タイムに使用されていることを示します。 このキーワードをコマンドに追加してもコマンドには影響がありませんが、コンフィギュレーションでこのコマンドを **failover polltime interface** コマンドと区別しやすくなります。

デフォルト

PIX セキュリティ アプライアンスのデフォルト値は次のとおりです。

- *poll_time* は 15 秒です。
- **holdtime** *time* は 45 秒です。

ASA セキュリティ アプライアンスのデフォルト値は次のとおりです。

- *poll_time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワードおよび **holdtime** キーワードが含まれるようになりました。
7.2(1)	**holdtime** キーワードに **msec** キーワードが追加されました。**polltime** の最小値が 500 ミリ秒から 200 ミリ秒に引き下げられました。**holdtime** の最小値が 3 秒から 800 ミリ秒に引き下げられました。

使用上のガイドライン

ユニットのポーリング タイムの 3 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要なスイッチオーバーが発生する可能性があります。

1 回のポーリング期間中にユニットがフェールオーバー通信インターフェイスまたはケーブルで hello パケットを受信しないと、残りのインターフェイス経由で追加のテストが行われます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

failover polltime [**unit**] コマンドおよび **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、ユニットのポーリング タイムの頻度を 3 秒に変更する例を示します。

```
hostname(config)# failover polltime 3
```

次に、200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒以内にフェールオーバー インターフェイスで hello パケットを受信しないとフェールオーバーを実行するようにセキュリティ アプライアンスを設定する例を示します。オプションの **unit** キーワードがコマンドに含まれています。

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

関連コマンド

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムおよびホールド タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover polltime interface

Active/Standby フェールオーバー コンフィギュレーションのデータ インターフェイスのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

構文の説明

holdtime *time*	（任意）データ インターフェイスが hello メッセージを受信する間隔を設定します。この時間を経過すると、ピアで障害が発生したと見なされます。有効な値は 5 ～ 75 秒です。
interface *time*	インターフェイス モニタリングのポーリング タイムを指定します。有効な値の範囲は、1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。

デフォルト

デフォルト値は次のとおりです。

- ポーリングの *time* は 5 秒です。
- **holdtime** *time* は、ポーリングの *time* の 5 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワード、**interface** キーワード、および **holdtime** キーワードが含まれるようになりました。
7.2(1)	オプションの **holdtime** *time* と、ミリ秒単位でポーリング タイムを指定する機能が追加されました。

使用上のガイドライン

データ インターフェイスで hello パケットが送信される頻度を変更するには、**failover polltime interface** コマンドを使用します。このコマンドは、Active/Standby フェールオーバーにのみ使用可能です。Active/Active フェールオーバーでは、**failover polltime interface** コマンドではなく、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。

ユニットのポーリング タイムの 5 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ホールド タイムの半分が経過したときに、インターフェイスで hello パケットが受信されていない場合は、インターフェイスのテストが開始されます。

failover polltime unit コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、インターフェイスのポーリング タイムの頻度を 15 秒に設定する例を示します。

```
hostname(config)# failover polltime interface 15
```

次に、インターフェイスのポーリング タイムの頻度を 500 ミリ秒に、ホールド タイムを 5 秒に設定する例を示します。

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

関連コマンド

コマンド	説明
failover polltime	装置のフェールオーバー ポーリング期間とホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover reload-standby

スタンバイ ユニットを強制的にリブートするには、特権 EXEC モードで **failover reload-standby** コマンドを使用します。

failover reload-standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイ ユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

例

次に、アクティブ ユニットで **failover reload-standby** コマンドを使用して、スタンバイ ユニットを強制的にリブートする例を示します。

```
hostname# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	実行コンフィギュレーションをスタンバイ ユニットのメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続のレプリケーションをイネーブルにするには、グローバル コンフィギュレーション モードで **failover replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

failover replication http

no failover replication http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドが、**failover replicate http** から **failover replication http** に変更されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用して、フェールオーバー グループごとに HTTP セッションのレプリケーションを制御します。

例

次に、HTTP 接続のレプリケーションをイネーブルにする例を示します。

```
hostname(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループに対して、HTTP セッションのレプリケーションをイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover reset

障害が発生したセキュリティ アプライアンスを障害が発生していない状態に復元するには、特権 EXEC モードで **failover reset** コマンドを使用します。

failover reset [**group** *group_id*]

構文の説明

group	（任意）フェールオーバー グループを指定します。**group** キーワードは、Active/Active フェールオーバーに対してのみ適用されます。
group_id	フェールオーバー グループの番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、オプションのフェールオーバー グループ ID を許可するように変更されました。

使用上のガイドライン

failover reset コマンドを使用すると、障害が発生したユニットまたはグループを、障害が発生していない状態に変更できます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブ ユニットでコマンドを入力することを推奨します。アクティブ ユニットで **failover reset** コマンドを入力すると、スタンバイ ユニットが障害が発生していない状態に復元されます。

show failover コマンドまたは **show failover state** コマンドを使用して、ユニットのフェールオーバー ステータスを表示できます。

このコマンドには、**no** 形式はありません。

Active/Active フェールオーバーでは、**failover reset** を入力すると、ユニット全体がリセットされます。コマンドにフェールオーバー グループを指定すると、指定したグループのみがリセットされます。

例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover timeout

非対称ルーテッド セッションのフェールオーバー再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

構文の説明

hh	タイムアウト値の時間を指定します。有効な値の範囲は、-1 ～ 1193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも接続を再開できます。 この値を 0 に設定し、他のタイムアウト値を指定しないと、コマンドがデフォルト値に設定されて再接続ができなくなります。**no failover timeout** コマンドを入力しても、この値がデフォルト（0）に設定されます。 **（注）** デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。
mm	（任意）タイムアウト値の分を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	（任意）タイムアウト値の秒を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトで、*hh*、*mm*、および *ss* は 0 であり、再接続はできないようになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コマンド リストに表示されるように変更されました。

使用上のガイドライン

このコマンドは、**nailed** オプションを指定した **static** コマンドとともに使用されます。**nailed** オプションを指定すると、起動後、またはシステムがアクティブになった後、指定した時間内に接続を再確立できます。**failover timeout** コマンドでは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドには影響しません。

（注）　**nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。

このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定します。

file-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [File Bookmarks] タイトルまたは [File Bookmarks] リンクをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **file-bookmarks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または CSS パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトル テキストは「File Folder Bookmarks」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、W3C の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[File Bookmarks] タイトルを「Corporate File Bookmarks」にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

file-browsing

ファイル サーバまたは共有の CIFS または FTP によるファイル ブラウジングをイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-browsing** コマンドを使用します。

file-browsing enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ファイル ブラウジングには、次の使用上の注意事項があります。

- ファイル ブラウジングでは、国際化はサポートされていません。
- ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードでファイル ブラウジングをディセーブルにした場合、セキュリティ アプライアンスはそれ以上値を検索しません。ディセーブルにする代わりに

file-browsing コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、セキュリティ アプライアンスはユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル ブラウジングをイネーブルにする例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-browsing enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

file-encoding

Common Internet File System サーバからのページの文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。file-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンス コンフィギュレーション内では、コマンド インタプリタによって大文字が小文字に変換されます。
server-ip-addr	文字エンコーディングを指定する CIFS サーバの IP アドレス（ドット付き 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバの名前。 セキュリティ アプライアンスでは、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

デフォルト

WebVPN コンフィギュレーションに明示的な file-encoding エントリがないすべての CIFS サーバからのページでは、character-encoding 属性の文字エンコーディング値が継承されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN の character-encoding 属性の値とは異なる文字エンコーディングが必要なすべての CIFS サーバに対して、file-encoding エントリを入力します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding 属性の値を符号化します。符号化が行われなかった場合は、character-encoding 属性の値を継承します。リモート ユーザのブラウザでは、ブラウザの文字エンコード セットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding 属性によって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォント ファミリを置換し、これらの値の設定を補足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。

例

次に、「CISCO-server-jp」という名前の CIFS サーバが日本語の Shift_JIS 文字をサポートするように file-encoding 属性を設定し、フォント ファミリを削除して、デフォルトの背景色を保持する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

次に、CIFS サーバ 10.86.5.174 の file-encoding 属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	WebVPN コンフィギュレーションの file-encoding エントリに指定されたサーバのページを除き、すべての WebVPN ポータル ページで使用されるグローバルな文字エンコーディングを指定します。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	Common Internet File System についてのデバッグ メッセージを表示します。

file-entry

アクセスするファイル サーバ名をユーザが入力できる機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-entry** コマンドを使用します。

file-entry enable | disable

enable | disable	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. 接続プロファイル（トンネル グループ）のグループ ポリシー
5. デフォルトのグループ ポリシー

属性の DAP 値には、ユーザ、グループ ポリシー、または接続プロファイルよりも高いプライオリティが設定されています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードでファイル サーバ名の入力をディセーブルにした場合、セキュリティ アプライアンスはそれ以上値を検索しません。ディセーブルにする代わりに **file-entry** コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、セキュリティ アプライアンスはユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル サーバ名の入力をイネーブルにする例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
```

```
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-entry enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-browsing	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

filter

特定のグループ ポリシーまたはユーザ名の WebVPN 接続で使用するアクセス リストの名前を指定するには、webvpn コンフィギュレーション モードで **filter** コマンドを使用します。アクセス リスト（**filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。

filter {**value** *ACLname* | **none**}

no filter

構文の説明

none	**WebVPN タイプ**のアクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

WebVPN アクセス リストは、**filter** コマンドを使用してアクセス リストを指定するまでは適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

no オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。その後、**filter** コマンドを使用して、これらの WebVPN トラフィック用の ACL を適用します。

WebVPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

例

次に、FirstGroup という名前のグループ ポリシーで *acl_in* という名前のアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

filter activex

セキュリティ アプライアンスを通過する HTTP トラフィック内の ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで **filter activex** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter activex | java **<***port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java **<***port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 21 の代わりに、**http** または **url** リテラルを使用できます。指定できる値の範囲は、0 ～ 65535 です。well-known ポートおよびそれらのリテラル値のリストについては、を参照してください。
-port	（任意）ポート範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ActiveX オブジェクトには、保護されているネットワーク上のホストやサーバを攻撃することを目的とするコードが含まれている場合があるため、セキュリティのリスクが発生する可能性があります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロールは、以前は OLE コントロールまたは OCX コントロールと呼ばれていたもので、Web ページやその他のアプリケーションに挿入できるコンポーネントです。これらのコントロールにはカスタム フォームやカレンダーなど、情報の収集と表示に使用されるサードパーティ製の多様なフォームが含まれています。ActiveX は、技術的に、ネットワーク クライアントに対して多くの問題を発生させる可能性があります。たとえば、ワークステーションの障害の原因となる、ネットワーク セキュリティ問題を引き起こす、またはサーバへの攻撃に利用される、などのおそれがあります。

filter activex コマンドでは、HTML Web ページ内で HTML の <object> コマンドをコメントアウトすることによって、<object> コマンドがブロックされます。<APPLET> ～ </APPLET> タグおよび <OBJECT CLASSID> ～ </OBJECT> タグを選択的にコメントに置換することによって、HTML ファイルの ActiveX フィルタリングが実行されます。ネストされたタグのフィルタリングは、最上位タグをコメントに変換することによってサポートされています。

注意　<object> タグは、Java アプレット、画像ファイル、およびマルチメディア オブジェクトにも使用されます。この場合、これらもこのコマンドによってブロックされます。

<object> または </object> HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、セキュリティ アプライアンスでタグをブロックできません。

alias コマンドによって参照されている IP アドレスにユーザがアクセスした場合、または WebVPN トラフィックでは、ActiveX ブロッキングは行われません。

例

次に、すべての発信接続で ActiveX オブジェクトをブロックする例を示します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、任意のローカル ホストから任意の外部ホストへの接続において、ポート 80 で Web トラフィックに対して ActiveX オブジェクト ブロッキングを適用することを指定します。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter ftp** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter ftp <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 80 の代わりに、**ftp** リテラルを使用できます。
-port	（任意）ポート範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
allow	（任意）サーバが利用できない場合に、フィルタリングなしで発信接続がセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
interact-block	（任意）ユーザが対話形式の FTP プログラムを使用して FTP サーバに接続することを禁止します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

filter ftp コマンドを使用すると、Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定できます。

この機能をイネーブルにした後、ユーザがサーバに対して FTP GET 要求を発行すると、セキュリティ アプライアンスは、FTP サーバ、および Websense サーバまたは N2H2 サーバに対して同時に要求を送信します。Websense サーバまたは N2H2 サーバによって接続が許可されると、セキュリティ アプライアンスは成功の FTP リターン コードを変更しないでそのままユーザに返します。たとえば、成功のリターン コードは「250: CWD command successful」です。

Websense サーバまたは N2H2 サーバによって接続が拒否されると、セキュリティ アプライアンスは FTP リターン コードを変更して、接続が拒否されたことを示します。たとえば、セキュリティ アプライアンスは、コード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します。Websense では、FTP GET コマンドのみがフィルタリングされ、FTP PUT コマンドはフィルタリングされません。

完全なディレクトリ パスを指定しない対話形式の FTP セッションを禁止するには、**interactive-block** オプションを使用します。対話形式の FTP クライアントを使用すると、ユーザは、完全なパスを入力しないでディレクトリを変更できます。たとえば、ユーザは、**cd /public/files** ではなく、**cd ./files** と入力できます。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次に、FTP フィルタリングをイネーブルにする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバまたは N2H2 サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

N2H2 サーバまたは Websense サーバでフィルタリングする HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter https** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、**https** リテラルを使用できます。
-port	（任意）ポート範囲を指定します。
except	（任意）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
allow	（任意）サーバが利用できない場合に、フィルタリングなしで発信接続がセキュリティ アプライアンスを通過します。このオプションを省略した場合に、N2H2 サーバまたは Websense サーバがオフラインになると、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバが再度オンラインになるまで、ポート 443 への発信トラフィックを停止します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、外部の Websense または N2H2 フィルタリング サーバを使用した HTTPS サイトおよび FTP サイトのフィルタリングをサポートしています。

サイトが許可されない場合、SSL 接続ネゴシエーションを完了させないことによって、HTTPS フィルタリングが行われます。ブラウザには、「The Page or the content cannot be displayed.」のようなエラーメッセージが表示されます。

HTTPS コンテンツは暗号化されているため、セキュリティ アプライアンスは、ディレクトリおよびファイル名の情報を付けずに URL ルックアップを送信します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで **filter java** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。
*port***-***port*	（任意）ポート範囲を指定します。
except	（任意）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Java アプレットは、保護されたネットワーク上のホストとサーバを攻撃するコードを含むことがあるため、セキュリティ リスクを引き起こす可能性があります。Java アプレットは、**filter java** コマンドで取り除くことができます。

filter java コマンドは、発信接続からセキュリティ アプライアンスに返される Java アプレットをフィルタリングします。フィルタリングされてもユーザは HTML ページを受信できますが、アプレットの Web ページ ソースはコメントアウトされているため、アプレットは実行できません。**filter java** コマンドでは、WebVPN トラフィックはフィルタリングされません。

applet または /applet HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、セキュリティ アプライアンスでタグをブロックできません。Java アプレットが <object> タグ内にあることがわかっている場合は、**filter activex** コマンドを使用して削除します。

例

次の例では、すべての発信接続で Java アプレットをブロックすることを指定しています。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドは、Java アプレット ブロックが、あらゆるローカル ホストからあらゆる外部ホストへのポート 80 の Web トラフィックに対して、適用されることを指定しています。

次の例では、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックしています。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドは、ホスト 192.168.3.3 による Java アプレットのダウンロードをブロックします。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

トラフィックを URL フィルタリング サーバに転送するには、グローバル コンフィギュレーション モードで **filter url** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

構文の説明

allow	サーバが利用できない場合、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
cgi_truncate	CGI スクリプトのように、URL に疑問符（?）から始まるパラメータ リストがある場合は、フィルタリング サーバに送信する URL から、疑問符を含む疑問符以降のすべての文字を削除します。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
http	ポート 80 を指定します。80 の代わりに **http** または **www** と入力してポート 80 を指定することもできます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超える場合や、URL バッファが使用できない場合に URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超える場合は、N2H2 サーバまたは Websense サーバに対して元のホスト名または IP アドレスのみを送信します。
mask	任意のマスク。
-port	（任意）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。ハイフンの後にもう 1 つポートを追加すると、ポートの範囲を指定できます。
proxy-block	ユーザの HTTP プロキシ サーバへの接続を禁止します。
url	セキュリティ アプライアンス経由で伝送されるデータから URL をフィルタリングします。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　**filter url** コマンドを使用すると、N2H2 または Websense フィルタリング アプリケーションを使用して指定した WWW 上の URL への発信ユーザのアクセスを禁止できます。

（注）　**filter url** コマンドを発行する前に、**url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションでは、N2H2 サーバまたは Websense サーバがオフラインになった場合のセキュリティ アプライアンスの動作が決定されます。**filter url** コマンドで **allow** オプションを使用し、N2H2 サーバまたは Websense サーバがオフラインになった場合、ポート 80 のトラフィックはフィルタリングなしでセキュリティ アプライアンスを通過します。**allow** オプションを指定しないでこのコマンドを使用し、サーバがオフラインになった場合、セキュリティ アプライアンスでは、サーバが再度オンラインになるまでポート 80（Web）への発信トラフィックが停止されるか、または別の URL サーバを使用できる場合は次の URL サーバに制御が渡されます。

（注）　**allow** オプションを設定した場合、セキュリティ アプライアンスでは、N2H2 サーバまたは Websense サーバがオフラインになると代替サーバに制御が渡されるようになりました。

N2H2 サーバまたは Websense サーバは、セキュリティ アプライアンスと連携して動作し、会社のセキュリティ ポリシーに基づいてユーザの Web サイトへのアクセスを拒否します。

フィルタリング サーバの使用方法

Websense プロトコル バージョン 4 では、ホストとセキュリティ アプライアンスとの間でのグループおよびユーザ名認証が可能です。セキュリティ アプライアンスは、ユーザ名ルックアップを実行し、その後 Websense サーバが URL フィルタリングおよびユーザ名のロギングを処理します。

N2H2 サーバは、IFP サーバを実行する Windows ワークステーション（2000、NT、または XP）である必要があります。512 MB 以上の RAM を推奨します。また、N2H2 サービスにおける長い URL のサポートは最大 3 KB までとなっており、Websense における制限よりも短くなっています。

Websense プロトコル バージョン 4 では、次の機能が拡張されました。

- URL フィルタリングにおいて、セキュリティ アプライアンスでは、Websense サーバに定義されているポリシーに対して発信 URL 要求をチェックできます。
- ユーザ名のロギングによって、Websense サーバでユーザ名、グループ、およびドメイン名が追跡されます。

- ユーザ名ルックアップによって、セキュリティ アプライアンスでは、ユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense についての情報は、次の Web サイトで入手できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の適切な形式の **url-server** コマンドを使用して、N2H2 サーバまたは Websense サーバを指定します。

ステップ 2　**filter** コマンドを使用して、フィルタリングをイネーブルにします。

ステップ 3　必要に応じて **url-cache** コマンドを使用して、スループットを向上させます。ただし、このコマンドは Websense ログを更新しないため、Websense アカウンティング レポートに影響がある可能性があります。**url-cache** コマンドを使用する前に、Websense の実行ログを蓄積します。

ステップ 4　**show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用して、実行情報を表示します。

長い URL の使用

Websense フィルタリング サーバでは 4 KB まで、N2H2 フィルタリング サーバでは 3 KB までの URL のフィルタリングがサポートされています。

許可されている最大サイズよりも長い URL 要求の処理を許可するには、**longurl-truncate** オプションおよび **cgi-truncate** オプションを使用します。

URL が最大長よりも長く、**longurl-truncate** オプションまたは **longurl-deny** オプションをイネーブルにしない場合、セキュリティ アプライアンスではパケットがドロップされます。

longurl-truncate オプションを指定すると、セキュリティ アプライアンスは URL が最大許容長よりも長い場合に、URL のホスト名または IP アドレス部分だけを、評価のためにフィルタリング サーバに送信します。**longurl-deny** オプションは、URL が最大許容長よりも長い場合、発信 URL トラフィックを拒否します。

パラメータは含まずに CGI スクリプトの場所とスクリプト名だけを含むよう CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機したり送信したりすると、大量のメモリ リソースが使用され、セキュリティ アプライアンスのパフォーマンスに影響を与える可能性があります。

HTTP 応答のバッファリング

デフォルトで、ユーザが特定の Web サイトに対する接続要求を発行すると、セキュリティ アプライアンスはその要求を Web サーバとフィルタリング サーバに同時に送信します。Web コンテンツ サーバよりも前にフィルタリング サーバが応答しない場合、Web サーバからの応答はドロップされます。このような場合、Web クライアントの観点からは、Web サーバの応答が遅延することになります。

HTTP 応答バッファをイネーブルにすることによって、Web コンテンツ サーバからの応答がバッファリングされ、フィルタリング サーバによって接続が許可された場合にその応答が要求元ユーザに転送されます。これにより、応答バッファをイネーブルにしない場合に発生する遅延を防止できます。

HTTP 応答バッファをイネーブルにするには、次のコマンドを入力します。

```
url-block block block-buffer-limit
```

block-buffer を、バッファリングする最大ブロック数で置き換えます。1 ～ 128 の値を指定できます。この値は、一度にバッファリング可能な 1550 バイトのブロック数を指定します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、ポート 8080 でリッスンするプロキシ サーバ宛てのすべての発信 HTTP 接続をブロックする例を示します。

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

FIPS に準拠するためのポリシー チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **fips enable** コマンドを使用します。ポリシー チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

fips enable

no fips enable

構文の説明

enable	FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 準拠動作モードで実行するには、**fips enable** コマンドを適用し、セキュリティ ポリシーに指定されている適切なコンフィギュレーションを適用する必要があります。内部 API によって、実行時に、適切なコンフィギュレーションが適用されるようにデバイスを移行できます。

スタートアップ コンフィギュレーションに「fips enable」が存在する場合は、FIPS POST が実行されて、次のコンソール メッセージが表示されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9
```

```
INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

例

次に、FIPS に準拠するためのポリシー チェックをシステムでイネーブルにする例を示します。

```
sw8-ASA(config)# fips enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

fips self-test poweron

電源オン セルフテストを実行するには、特権 EXEC モードで **fips self-test powereon** コマンドを使用します。

fips self-test poweron

構文の説明

poweron	電源オン セルフテストを実行します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、デバイスで、FIPS 140-2 準拠に必要なすべてのセルフテストが実行されます。テストには、暗号化アルゴリズム テスト、ソフトウェア完全性テスト、および重要機能のテストがあります。

例

次に、システムで電源オン セルフテストを実行する例を示します。

```
sw8-5520(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードをトランスペアレント モードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 のファイアウォールであり、接続デバイスにはルータ ホップとして認識されません。

firewall transparent

no firewall transparent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードのみを使用できます。モードは、システム コンフィギュレーションで設定する必要があります。このコマンドは、各コンテキストのコンフィギュレーションにも情報提供の目的で表示されますが、このコマンドをコンテキストで入力することはできません。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、セキュリティ アプライアンスによってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。

firewall transparent コマンドを使用してモードを変更するテキスト コンフィギュレーションをセキュリティ アプライアンスにダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、セキュリティ アプライアンスでこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。コマンドをコンフィギュレーションの後の方に配置すると、コンフィギュレーション内のその位置よりも前にあるすべての行がセキュリティ アプライアンスによってクリアされます。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
hostname(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを表示します。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

flowcontrol

フロー制御のポーズ（XOFF）フレームを 10 ギガビット イーサネット インターフェイスでのみイネーブルにするには、インターフェイス コンフィギュレーション モードで **flowcontrol** コマンドを使用します。ポーズ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

構文の説明

low_water	低基準値を 0 ～ 511 KB の範囲で設定します。Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）からポーズ フレームが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。デフォルトは、64 KB です。
pause_time	ポーズ リフレッシュのしきい値を 0 ～ 65535 の範囲で設定します。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のこのタイマー値によって制御されます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。デフォルトは 26624 です。
noconfirm	確認なしでコマンドを適用します。このコマンドでは、インターフェイスがリセットされるため、このオプションを指定しない場合は、コンフィギュレーションの変更の確認を求められます。
high_water	高基準値を 0 ～ 511 KB の範囲で設定します。バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。デフォルトは 128 KB です。

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ポーズ フレームは、デフォルトではディセーブルになっています。

デフォルトの最高水準点は 128 KB です。

デフォルトの最低水準点は 64 KB です。

デフォルトのポーズ リフレッシュのしきい値は 26664 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、物理インターフェイスに対して入力します。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。

このコマンドをイネーブルにすると、FIFO バッファの使用量に基づいて、NIC ハードウェアによってポーズ（XOFF）フレームおよび XON フレームが自動的に生成されます。

1. バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。
2. ポーズが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。
3. リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。
4. バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが NIC から繰り返し送信されます。

このコマンドを使用すると、次の警告が表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

（注） 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティ ベースのフロー制御はサポートされていません。

例

次に、デフォルト設定を使用してポーズ フレームをイネーブルにする例を示します。

```
hostname(config)# interface tengigabitethernet 1/0
hostname(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
hostname(config-if)# y
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

format

すべてのファイルを消去してファイル システムをフォーマットするには、特権 EXEC モードで **format** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

format {**disk0: | disk1: | flash:**}

構文の説明

disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

format コマンドは、指定したファイル システム上のすべてのデータを消去して、デバイスに FAT 情報を再書き込みします。

注意　**format** コマンドは、破損したフラッシュ メモリをクリーン アップするために必要な場合にのみ、細心の注意を払って使用してください。

（非表示のシステム ファイルを除く）表示されているすべてのファイルを削除する場合は、**format** コマンドではなく **delete /recursive** コマンドを入力します。

（注）　Cisco PIX セキュリティ アプライアンスでは、**erase** コマンドおよび **format** コマンドは両方とも、0xFF パターンを使用してユーザ データを破棄します。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** を入力します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** を入力します。

例

次に、フラッシュ メモリをフォーマットする方法の例を示します。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

forward interface

ASA 5505 適応型セキュリティ アプライアンスなどの組み込みのスイッチを備えたモデルにおいて、特定の VLAN で他の特定の VLAN への接続の開始を可能にするには、インターフェイス コンフィギュレーション モードで **forward interface** コマンドを使用します。特定の VLAN で他の特定の VLAN への接続が開始されないよう制限するには、このコマンドの **no** 形式を使用します。ライセンスでサポートされている VLAN 数に応じて、特定の VLAN の制限が必要となることがあります。

forward interface vlan *number*

no forward interface vlan *number*

構文の説明

vlan *number*	この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

デフォルト

デフォルトでは、すべてのインターフェイスから他のすべてのインターフェイスにトラフィックを開始できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。いずれのライセンスでも、ASA 5505 適応型セキュリティ アプライアンスでは最大 5 つの非アクティブな VLAN を設定できますが、これらをアクティブにする場合は、ライセンスのガイドラインに従う必要があります。

基本ライセンスでは、3 つめの VLAN は **no forward interface** コマンドを使用して設定し、この VLAN から他の特定の VLAN への接続の開始を制限する必要があります。

たとえば、1 つめの VLAN がインターネット アクセス用の外部ネットワークに、2 つめの VLAN が内部の業務用ネットワークに、3 つめの VLAN が家庭用ネットワークにそれぞれ割り当てられているとします。家庭用ネットワークから業務用ネットワークにアクセスする必要はないため、家庭用 VLAN に対して **no forward interface** コマンドを使用できます。業務用ネットワークから家庭用ネットワークにはアクセスできますが、家庭用ネットワークから業務用ネットワークにはアクセスできません。

すでに 2 つの VLAN インターフェイスに **nameif** コマンドを設定している場合は、3 つめのインターフェイスに **nameif** コマンドを設定する前に **no forward interface** コマンドを入力する必要があります。セキュリティ アプライアンス（ASA 5505 適応型セキュリティ アプライアンス）の基本ライセンスでは、3 つの VLAN インターフェイスすべてを完全に動作させることは許可されていません。

例

次の例では、3 つの VLAN インターフェイスを設定します。3 つめの家庭用インターフェイスは、業務用インターフェイスにトラフィックを転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
backup interface	たとえば、ISP へのバックアップ リンクとしてインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

fqdn

登録時に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **fqdn** コマンドを使用します。fqdn のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

fqdn [*fqdn* | **none**]

no fqdn

構文の説明

fqdn	完全修飾ドメイン名を指定します。*fqdn* の最大長は 64 文字です。
none	完全修飾ドメイン名を指定しません。

デフォルト

デフォルトの設定には、FQDN は含まれていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

証明書を使用した Nokia VPN クライアントの認証をサポートするようにセキュリティ アプライアンスを設定する場合は、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証のサポートの詳細については、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に FQDN engineering を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

fragment

パケット フラグメンテーションの付加的な管理を提供して、NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで **fragment** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

構文の説明

chain *limit*	完全な IP パケットをフラグメント化できる最大フラグメント数を指定します。
interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。
size *limit*	IP 再構築データベース内で再構築を待機可能な最大フラグメント数を設定します。 **（注）** セキュリティ アプライアンスでは、キューのサイズが 2/3 までいっぱいになると、既存のファブリック チェーンの一部ではないすべてのフラグメントが受け入れられなくなります。キューの残りの 1/3 は、すでに部分的にキューイングされている不完全なフラグメント チェーンと送信元 IP アドレス、宛先 IP アドレス、および IP ID 番号が同じであるフラグメントを受け入れるために使用されます。この制限は、フラグメント フラッディング攻撃が行われた場合でも、正規のフラグメント チェーンの再構築を可能にするための DoS 保護メカニズムです。
timeout *limit*	フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

デフォルト

デフォルトの設定は次のとおりです。

- **chain** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- **size** は 200 です。
- **timeout** は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドの引数が変更されました。**chain**、**size**、または **timeout** のいずれかの引数を選択する必要があります。ソフトウェアの以前のリリースではこれらの引数なしで **fragment** コマンドを入力できましたが、これらの引数なしでは入力できなくなりました。

使用上のガイドライン

デフォルトで、セキュリティ アプライアンスでは、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスで **fragment chain 1** *interface* コマンドを入力して、フラグメント化されたパケットがセキュリティ アプライアンスを通過しないようにセキュリティ アプライアンスを設定することを検討する必要があります。limit を 1 に設定すると、すべてのパケットは完全なものである必要があります。つまり、フラグメント化されていない必要があります。

セキュリティ アプライアンスを通過するネットワーク トラフィックの多くが NFS である場合は、データベースのオーバーフローを回避するために追加の調整が必要となることがあります。

WAN インターフェイスなど、NFS サーバとクライアントとの間の MTU サイズが小さい環境では、**chain** キーワードに追加の調整が必要となる場合があります。この場合、効率性を向上させるために、NFS over TCP を使用することを推奨します。

size *limit* を大きな値に設定すると、セキュリティ アプライアンスがフラグメント フラッディングによる DoS 攻撃を受けやすくなります。**size** *limit* の値は、1550 または 16384 プールの合計ブロック数 以上には設定しないでください。

デフォルト値を使用すると、フラグメント フラッディングによる DoS 攻撃が抑制されます。

例

次に、外部インターフェイスおよび内部インターフェイスにおいてフラグメント化されたパケットの通過を禁止する例を示します。

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

引き続き、フラグメント化されたパケットの通過を禁止する追加の各インターフェイスに対して、**fragment chain 1** *interface* コマンドを入力します。

次に、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェーン長 45、待機時間 10 秒に設定する例を示します。

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA 動作の反復間隔を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **frequency** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

frequency *seconds*

no frequency

構文の説明

seconds	SLA プローブ間の秒数。有効な値は、1 ～ 604800 秒です。この値は、**timeout** の値未満にはできません。

デフォルト

デフォルトの頻度は、60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA 動作は、動作のライフタイム中、指定された頻度で繰り返し実行されます。たとえば、60 秒の頻度に設定された **ipIcmpEcho** 動作は、動作のライフタイム中 60 秒ごとにエコー要求パケットを繰り返し送信します。たとえば、エコー動作のデフォルトのパケット数は 1 です。動作が開始されるとこのパケットが送信され、60 秒後に再度送信されます。

個別の SLA 動作において、指定された頻度の値よりも実行に時間がかかる場合は、動作がすぐに繰り返されるのではなく、「busy」という統計情報カウンタが増加します。

frequency コマンドには、**timeout** コマンドに指定された値未満の値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度が 3 秒に、タイムアウト値が 1000 ミリ秒に設定されています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

fsck

ファイル システムのチェックを実行して、破損を修復するには、特権 EXEC モードで **fsck** コマンドを使用します。

fsck [/no confirm]{disk0: | disk1: | flash:}

構文の説明

/noconfirm	任意。修復確認のためのプロンプトを表示しません。
disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

fsck コマンドは破損したファイル システムをチェックし、修復を試みます。他の方法を用いる前に、まずこのコマンドを使用してください。

/noconfirm キーワードは、最初に確認を求めずに破損を自動的に修復します。

例

次の例では、フラッシュ メモリのファイル システムのチェック方法を示しています。

```
hostname# fsck flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで **ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モードにリセットするには、このコマンドの **no** 形式を使用します。

ftp mode passive

no ftp mode passive

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。セキュリティ アプライアンスでは、FTP を使用して、FTP サーバとの間でイメージ ファイルやコンフィギュレーション ファイルをアップロードまたはダウンロードできます。**ftp mode passive** コマンドは、セキュリティ アプライアンス上の FTP クライアントの FTP サーバとの通信方法を制御します。

パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードとはサーバの状態を指しており、クライアントが開始する制御接続およびデータ接続の両方をサーバが受動的に受け入れることを意味しています。

パッシブ モードでは、送信元ポートおよび宛先ポートの両方が 1023 よりも大きい一時ポートです。モードはクライアントによって設定されます。クライアントは、**passive** コマンドを発行して、パッシブ データ接続の設定を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

例

次に、FTP モードをパッシブに設定する例を示します。

```
hostname(config)# ftp mode passive
```

関連コマンド

copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。

debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions（削除）

functions コマンドは、リリース 8.0(2) では使用できません。このコマンドは廃止されており、下位互換性の目的でのみこのコマンド リファレンスに記載されています。Web サイトの URL リストの作成、ファイル アクセス、プラグイン、カスタマイゼーション、言語変換には、import コマンドおよび export コマンドを使用します。

特定のユーザまたはグループ ポリシーに対して、ポート フォワーディング Java アプレットの自動ダウンロード、ファイル アクセス、ファイル ブラウジング、ファイル サーバ名の入力、Web タイプ ACL の適用、HTTP プロキシ、ポート フォワーディング、または WebVPN 上での URL 入力を設定するには、webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定済みの機能を削除するには、このコマンドの **no** 形式を使用します。

functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none**}

no functions [**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **url-entry** | **port-forward**]

構文の説明

auto-download	WebVPN ログイン時のポート フォワーディング Java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初に、ポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	リモート ユーザに対して、MetaFrame Application Server からのターミナル サービスのサポートをイネーブルまたはディセーブルにします。このキーワードを指定すると、セキュリティ アプライアンスがセキュアな Citrix コンフィギュレーション内でセキュア ゲートウェイとして動作します。これらのサービスでは、ユーザは、標準的な Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN ホームページには、サーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル サーバ名の入力をイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ユーザによるファイル サーバ名の入力を許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザによるファイル サーバの名前の入力をイネーブルまたはディセーブルにします。
filter	Web タイプ ACL を適用します。イネーブルの場合、セキュリティ アプライアンスは、WebVPN の **filter** コマンドで定義された Web タイプ ACL を適用します。

http-proxy	リモート ユーザへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、Java、ActiveX、Flash などの、適切なマングリングに対して干渉するテクノロジーにおいて有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
none	すべての WebVPN **functions** に対してヌル値を設定します。デフォルトまたは指定したグループ ポリシーから機能を継承しません。
port-forward	ポート フォワーディングをイネーブルにします。イネーブルの場合、セキュリティ アプライアンスは、WebVPN の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	ユーザによる URL の入力をイネーブルまたはディセーブルにします。イネーブルの場合でも、セキュリティ アプライアンスは引き続き設定されている URL またはネットワーク ACL に基づいて URL を制限します。URL 入力がディセーブルの場合、セキュリティ アプライアンスでは、WebVPN ユーザは、ホームページ上の URL に制限されます。

デフォルト

機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは廃止されました。
7.1(1)	auto-download キーワードおよび citrix キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

functions none コマンドを発行することによって作成されたヌル値を含め、設定されているすべての機能を削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。機能の値を継承しない場合は、**functions none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、ファイル アクセスおよびファイル ブラウジングを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

CHAPTER 13

gateway コマンド～ hw-module module shutdown コマンド

gateway

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

構文の説明

gateway	特定のゲートウェイを管理しているコール エージェントのグループを指定します。
ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、**gateway** コマンドを使用します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

global

NAT 用にマッピング先のアドレスのプールを作成するには、グローバル コンフィギュレーション モードで **global** コマンドを使用します。アドレスのプールを削除するには、このコマンドの **no** 形式を使用します。

global (*mapped_ifc) nat_id* {*mapped_ip*[**-***mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[**-***mapped_ip*] [**netmask** *mask*] | **interface**}

構文の説明

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。インターフェイス アドレスを使用する必要がある場合はこのキーワードを使用しますが、アドレスは、DHCP を使用してダイナミックに割り当てられます。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip[**-***mapped_ip*]	マッピングされているインターフェイスから出るときに実アドレスの変換先となる、マッピング先のアドレス（複数可）を指定します。単一のアドレスを指定する場合は、PAT を設定します。アドレスの範囲を指定する場合は、ダイナミック NAT を設定します。 外部ネットワークがインターネットに接続されている場合は、各グローバル IP アドレスが Network Information Center（NIC）に登録されている必要があります。
nat_id	NAT ID の整数を指定します。この ID は、変換対象の実アドレスにマッピング プールを関連付けるために、**nat** コマンドによって参照されます。 通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（**nat id access-list**）の場合、整数の範囲は 1 ～ 65535 となります。 NAT ID 0 に対して **global** コマンドを指定しないでください。0 は、アイデンティティ NAT および NAT 免除用に予約されており、これらの NAT では **global** コマンドは使用しません。
netmask *mask*	（任意）*mapped_ip* のネットワーク マスクを指定します。このマスクは、*mapped_ip* と組み合わせた場合にはネットワークを指定しません。この場合は *mapped_ip* をホストに割り当てるときに *mapped_ip* に割り当てたサブネット マスクを指定します。アドレスの範囲を設定する場合は、*mapped_ip-mapped_ip* を指定する必要があります。 マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、1 つの **global** コマンドと一致します。

ダイナミック NAT および PAT の詳細については、**nat** コマンドを参照してください。

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
```

```
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
clear configure global	**global** コマンドをコンフィギュレーションから削除します。
nat	変換対象となる実アドレスを指定します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。
static	1 対 1 の変換を設定します。

group-alias

ユーザがトンネル グループの参照に使用する 1 つ以上の変換名を作成するには、トンネル グループ webvpn コンフィギュレーション モードで **group-alias** コマンドを使用します。リストからエイリアスを削除するには、このコマンドの **no** 形式を使用します。

group-alias *name* [**enable** | **disable]**

no group-alias *name*

構文の説明

disable	グループ エイリアスをディセーブルにします。
enable	以前ディセーブルにしたグループ エイリアスをイネーブルにします。
name	トンネル グループ エイリアスの名前を指定します。選択した任意のストリングを指定できます。ただし、スペースを含めることはできません。

デフォルト

デフォルトのグループ エイリアスはありませんが、グループ エイリアスを指定すると、そのエイリアスがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ここで指定したグループ エイリアスが、ログイン ページのドロップダウン リストに表示されます。各グループに複数のエイリアスを指定することも、エイリアスを指定しないことも可能です。このコマンドは、同じグループが「Devtest」や「QA」などの複数の一般名で知られている場合に役立ちます。

例

次に、「devtest」という名前の webvpn トンネル グループを設定し、そのグループに対してエイリアス「QA」および「Fra-QA」を確立するコマンドの例を示します。

```
hostname(config)# tunnel-group devtest type webvpn
hostname(config)# tunnel-group devtest webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias QA
hostname(config-tunnel-webvpn)# group-alias Fra-QA
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ設定をクリアします。
show webvpn group-alias	指定したトンネル グループまたはすべてのトンネル グループのエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定するためのトンネル グループ webvpn コンフィギュレーション モードを開始します。

group-delimiter

グループ名の解析をイネーブルにして、トンネルのネゴシエート時に受信したユーザ名からグループ名を解析する場合に使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名解析をディセーブルにするには、このコマンドの **no** 形式を使用します。

group-delimiter *delimiter*

no group-delimiter

構文の説明

delimiter	グループ名のデリミタとして使用する文字を指定します。 有効な値は、**@**、**#**、および **!** です。

デフォルト

デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デリミタは、トンネルがネゴシエートされるときに、ユーザ名からトンネル グループ名を解析するために使用されます。デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

例

次に、グループ デリミタをハッシュ マスク（#）に変更する **group-delimiter** コマンドの例を示します。

```
hostname(config)# group-delimiter #
```

関連コマンド

コマンド	説明
clear configure group-delimiter	設定したグループ デリミタをクリアします。
show running-config group-delimiter	現在のグループ デリミタ値を表示します。
strip-group	グループ除去処理をイネーブルまたはディセーブルにします。

group-lock

リモート ユーザがトンネル グループを介してしかアクセスできないように制限するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **group-lock** コマンドを発行します。

実行コンフィギュレーションから **group-lock** 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

構文の説明

none	group-lock をヌル値に設定します。これにより、グループ ロックの制限が許可されなくなります。デフォルトまたは指定したグループ ポリシーの group-lock 値を継承しないようにします。
value *tunnel-grp-name*	ユーザが接続する際にセキュリティ アプライアンスによって要求される既存のトンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—
ユーザ名コンフィギュレーション	•	—	•	—	—

使用上のガイドライン

グループ ロックをディセーブルにするには、**group-lock none** コマンドを使用します。

グループ ロックは、VPN クライアントに設定されているグループが、ユーザが割り当てられているトンネル グループと同一であるかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、セキュリティ アプライアンスはユーザによる接続を禁止します。グループ ロックを設定しなかった場合、セキュリティ アプライアンスは、割り当てられているグループに関係なくユーザを認証します。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーにグループ ロックを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

ネットワーク オブジェクト グループを追加するには、プロトコル、ネットワーク、サービス、および ICMP タイプ コンフィギュレーション モードで **group-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

group-object *obj_grp_id*

no group-object *obj_grp_id*

構文の説明

obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プロトコル、ネットワーク、サービス、ICMP タイプ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

group-object コマンドは、それ自身がオブジェクト グループであるオブジェクトを定義するために、**object-group** コマンドとともに使用します。このコマンドは、プロトコル、ネットワーク、サービス、および ICMP タイプ コンフィギュレーション モードで使用します。このサブコマンドを使用すると、同じタイプのオブジェクトを論理グループ化して、構造化されたコンフィギュレーションの階層オブジェクト グループを構築できます。

オブジェクト グループ内でのオブジェクトの重複は、それらのオブジェクトがグループ オブジェクトの場合は許可されます。たとえば、オブジェクト 1 がグループ A とグループ B の両方に存在する場合、A と B の両方を含むグループ C を定義できます。ただし、グループの階層が循環型になるようなグループ オブジェクトを含めることはできません。たとえば、グループ A にグループ B を含め、さらにグループ B にグループ A を含めることはできません。

階層オブジェクト グループは 10 レベルまで許可されています。

（注） セキュリティ アプライアンスでは IPv6 のネスト化したオブジェクト グループはサポートしていません。このため、そのようなグループ内に属する IPv6 エンティティを持つオブジェクトが別の IPv6 オブジェクト グループに含まれる場合、このオブジェクトに対しては **group-object** コマンドを使用できません。

例

次に、ネットワーク コンフィギュレーション モードで **group-object** コマンドを使用して、ホストを重複させる必要性を排除する例を示します。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

group-policy

グループ ポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

構文の説明

external server-group *server_group*	グループ ポリシーを外部として指定し、セキュリティ アプライアンスが属性を照会する AAA サーバ グループを識別します。
from *group-policy_name*	この内部グループ ポリシーの属性を、既存のグループ ポリシーの値に初期化します。
internal	グループ ポリシーを内部として識別します。
name	グループ ポリシーの名前を指定します。この名前は最大 64 文字で、スペースを含めることができます。スペースを含むグループ名は、二重引用符で囲む必要があります（"Sales Group" など）。
password *server_password*	外部 AAA サーバ グループから属性を取得する際に使用するパスワードを指定します。パスワードは最大 128 文字です。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスには、「DefaultGroupPolicy」という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するようにセキュリティ アプライアンスを設定しない限り、有効ではありません。設定手順については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

group-policy attributes コマンドを使用して設定グループ ポリシー モードを開始します。このモードでは、グループ ポリシーのあらゆる属性値ペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

また、設定グループ ポリシーモードで **webvpn** コマンドを入力するか、**group-policy attributes** コマンドを入力してから、設定グループ webvpn モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn モード属性を設定できます。詳細については、**group-policy attributes** コマンドの説明を参照してください。

例

次に、「FirstGroup」という名前の内部グループ ポリシーを作成する例を示します。

```
hostname(config)# group-policy FirstGroup internal
```

次に、AAA サーバ グループ「BostonAAA」およびパスワード「12345678」を指定して、「ExternalGroup」という名前の外部グループ ポリシーを作成する例を示します。

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

group-policy attributes

設定グループ ポリシー モードを開始するには、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを使用します。グループ ポリシーからすべての属性を削除するには、このコマンドの **no** バージョンを使用します。設定グループ ポリシー モードでは、指定したグループ ポリシーの属性値ペアを設定したり、グループ ポリシー webvpn コンフィギュレーション モードを開始してグループの webvpn 属性を設定したりできます。

group-policy *name* **attributes**

no group-policy *name* **attributes**

構文の説明

name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

属性モードのコマンド構文には、一般的に、次のような特徴があります。

- **no** 形式は実行コンフィギュレーションから属性を削除し、別のグループ ポリシーからの値の継承をイネーブルにします。
- **none** キーワードは実行コンフィギュレーションの属性をヌル値に設定し、これによって継承を禁止します。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

セキュリティ アプライアンスには、DefaultGroupPolicy という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するようにセキュリティ アプライアンスを設定しない限り、有効ではありません。設定手順については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

group-policy attributes コマンドを使用して設定グループ ポリシー モードを開始します。このモードでは、グループ ポリシーのあらゆる属性値ペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

また、**group-policy attributes** コマンドを入力してから、設定グループ ポリシー モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn モード属性を設定できます。詳細については、**webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）の説明を参照してください。

例

次に、FirstGroup という名前のグループ ポリシーのグループ ポリシー属性モードを開始する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成、編集、または削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn（グループ ポリシー属性モード）	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

group-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される WebVPN ページ ログイン ボックスのグループ プロンプトをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **group-prompt** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

グループ プロンプトのデフォルト テキストは「GROUP:」です。

グループ プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、テキストを「Corporate Group:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# group-prompt text Corporate Group:
F1-asa1(config-webvpn-custom)# group-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

group-search-timeout

show ad-groups コマンドを使用して照会した Active Directory サーバからの応答を待機する最大時間を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

group-search-timeout *seconds*

no group-search-timeout *seconds*

構文の説明

seconds	Active Directory サーバからの応答を待機する時間（1 ～ 300 秒）。

デフォルト

デフォルトは 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは LDAP を使用している Active Directory サーバにのみ適用され、Active Directory サーバでリストされているグループが表示されます。**group-search-timeout** コマンドを使用して、サーバからの応答を待機する時間を調整します。

例

次に、タイムアウトを 20 秒に設定する例を示します。

```
hostname(config-aaa-server-host)#group-search-timeout 20
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

group-url

グループに対する着信 URL または IP アドレスを指定するには、トンネル グループ webvpn コンフィギュレーション モードで **group-url** コマンドを使用します。リストから URL を削除するには、このコマンドの **no** 形式を使用します。

group-url *url* [**enable** | **disable**]

no group-url *url*

構文の説明

disable	URL をディセーブルにしますが、リストからは削除しません。
enable	URL をイネーブルにします。
url	このトンネル グループの URL または IP アドレスを指定します。

デフォルト

デフォルトの URL または IP アドレスはありませんが、URL または IP アドレスを指定すると、これがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

グループの URL または IP アドレスを指定すると、ユーザがログイン時にグループを選択する必要がなくなります。ユーザがログインすると、セキュリティ アプライアンスはトンネル グループ ポリシー テーブル内でユーザの着信 URL/アドレスを検索します。URL/アドレスが見つかり、さらにトンネル グループで group-url がイネーブルになっている場合、セキュリティ アプライアンスは関連するトンネル グループを自動的に選択して、ユーザ名およびパスワード フィールドだけをログイン ウィンドウでユーザに表示します。これによりユーザ インターフェイスが簡素化され、グループ リストがユーザに表示されなくなるという利点が追加されます。ユーザに表示されるログイン ウィンドウでは、そのトンネル グループ用に設定されているカスタマイゼーションが使用されます。

URL/アドレスがディセーブルで、group-alias が設定されている場合は、グループのドロップダウン リストも表示され、ユーザによる選択が必要になります。

1 つのグループに対して複数の URL/アドレスを設定する（または、1 つも設定しない）ことができます。URL/アドレスごとに個別にイネーブルまたはディセーブルに設定できます。指定した URL/アドレスごとに個別の **group-url** コマンドを使用する必要があります。http または https プロトコルを含めて、URL/アドレス全体を指定する必要があります。

複数のグループに同じ URL/アドレスを関連付けることはできません。セキュリティ アプライアンスでは、URL/アドレスの一意性を検証してから、トンネル グループに対する URL/アドレスを受け入れます。

次に、「test」という名前の webvpn トンネル グループを設定して、「http://www.cisco.com」および「https://supplier.com」という 2 つのグループ URL をそのグループ用に確立する例を示します。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com
hostname(config-tunnel-webvpn)# group-url https://supplier.company.com
hostname(config-tunnel-webvpn)#
```

次に、RadiusServer という名前のトンネル グループに対して、グループ URL、http://www.cisco.com および http://192.168.10.10 をイネーブルにする例を示します。

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ設定をクリアします。
show webvpn group-url	指定したトンネル グループまたはすべてのトンネル グループの URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

h245-tunnel-block

H.323 で H.245 トンネリングをブロックするには、パラメータ コンフィギュレーション モードで **h245-tunnel-block** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

h245-tunnel-block action [drop-connection | log]

no h245-tunnel-block action [drop-connection | log]

構文の説明

drop-connection	H.245 トンネルが検出された場合、コール設定接続をドロップします。
log	H.245 トンネルが検出された場合、ログを発行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 コールで H.245 トンネリングをブロックする例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# h245-tunnel-block action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hello-interval

インターフェイス上で送信される EIGRP hello パケット間の間隔を指定するには、インターフェイス コンフィギュレーション モードで **hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

デフォルト

デフォルトの *seconds* は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hold-time	hello パケットでアドバタイズされる EIGRP ホールド タイムを設定します。

help

指定するコマンドのヘルプ情報を表示するには、ユーザ EXEC モードで **help** コマンドを使用します。

help {*command* | **?**}

構文の説明

command	CLI ヘルプを表示するコマンドを指定します。
?	現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

help コマンドを使用すると、すべてのコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定せず、その代わりに **?** と 入力した場合、現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。

pager コマンドがイネーブルの場合、24 行表示されると、リスト表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトでは、次のように、UNIX の **more** コマンドに類似した構文が使用されます。

- 次のテキスト画面を表示するには、Space バーを押します。
- 次の行を表示するには、Enter キーを押します。
- コマンドラインに戻るには、q キーを押します。

例

次に、**rename** コマンドのヘルプを表示する例を示します。

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>
```

```
DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

次に、コマンド名と疑問符を入力して、ヘルプを表示する例を示します。

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コマンド プロンプトで **?** を入力すると、主要コマンド（**show**、**no**、または **clear** コマンド以外）に関する ヘルプを表示できます。

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

hic-fail-group-policy（非推奨）

グループ ポリシーを指定して、デフォルト グループ ポリシーとは異なる WebVPN ユーザ アクセス権限を取得するには、トンネル グループ webvpn コンフィギュレーション モードで **hic-fail-group-policy** コマンドを使用します。このコマンドの **no** 形式を使用すると、グループ ポリシーがデフォルト グループ ポリシーに設定されます。

hic-fail-group-policy *name*

no hic-fail-group-policy

構文の説明

name	グループ ポリシーの名前を指定します。

デフォルト

DfltGrpPolicy

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、Cisco Secure Desktop がインストールされているセキュリティ アプライアンスにのみ有効です。*システム検知*とも呼ばれるホストの整合性チェックには、VPN 機能ポリシーを適用するために満たす必要がある最小セットの基準がリモート PC に備わっているかどうかのチェックが含まれています。セキュリティ アプライアンスは、次のように hic-fail-group-policy 属性の値を使用して、リモート CSD ユーザへのアクセス権限を制限します。

- VPN 機能ポリシーを「Use Failure Group-Policy」に設定している場合は、常にこの値を使用します。
- VPN 機能ポリシーを「Use Success Group-Policy, if criteria match」に設定している場合は、基準が一致しなかったときに、この値を使用します。

この属性は、適用される失敗グループ ポリシーの名前を指定します。グループ ポリシーを使用して、アクセス権限を、デフォルト グループ ポリシーに関連付けられているアクセス権限と区別します。

（注） VPN 機能ポリシーを「Always use Success Group-Policy」に設定している場合、セキュリティ アプライアンスではこの属性を使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

例

次に、「FirstGroup」という名前の WebVPN トンネル グループを作成して、「group2」という名前の失敗グループ ポリシーを指定する例を示します。

```
hostname(config)# tunnel-group FirstGroup webvpn
hostname(config)# tunnel-group FirstGroup webvpn-attributes
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	指定したトンネル グループの WebVPN 属性を指定します。

hidden-parameter

セキュリティ アプライアンスが SSO 認証のために認証 Web サーバに送信する HTTP POST 要求の非表示パラメータを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **hidden-parameter** コマンドを使用します。実行コンフィギュレーションからすべての非表示パラメータを削除するには、このコマンドの **no** 形式を使用します。

hidden-parameter *string*

no hidden-parameter

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	フォームに組み込まれて SSO サーバに送信される非表示パラメータ。複数行に入力できます。各行の最大文字数は 255 です。すべての行をあわせた（非表示パラメータ全体の）最大文字数は 2048 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

これは HTTP フォームのコマンドを使用した SSO です。

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、認証 Web サーバにシングル サインオン認証要求を送信します。その要求では、ユーザには表示されない SSO HTML フォームの特定の非表示パラメータ（ユーザ名およびパスワード以外）が必要になることがあります。Web サーバから受信したフォームに対して HTTP ヘッダー アナライザを使用することで、Web サーバが POST 要求で想定している非表示パラメータを検出できます。

コマンド **hidden-parameter** を使用すると、Web サーバが認証 POST 要求で必要としている非表示パラメータを指定できます。ヘッダー アナライザを使用する場合は、エンコーディング済みの URL パラメータを含む非表示パラメータ ストリング全体をコピーして貼り付けることができます。

入力を簡単にするために、複数の連続行で非表示パラメータを入力できます。セキュリティ アプライアンスでは、その複数行を連結して単一の非表示パラメータにします。非表示パラメータ 1 行ごとの最大文字数は 255 文字ですが、各行にはそれより少ない文字しか入力できません。

（注）　ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、& で区切られた 4 つのフォーム エントリとその値で構成される非表示パラメータの例を示します。POST 要求から抜き出された 4 つのエントリおよびその値は、次のとおりです。

- SMENC、値は ISO-8859-1
- SMLOCALE、値は US-EN
- ターゲット、値は https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason、値は 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

hidden-shares

CIFS ファイルの非表示共有の可視性を制御するには、設定グループ webvpn コンフィギュレーション モードで **hidden-shares** コマンドを使用します。非表示共有オプションをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

hidden-shares {none | visible}

[no] hidden-shares {none | visible}

構文の説明

none	設定済みの非表示共有の表示およびアクセスをユーザが実行できないことを指定します。
visible	非表示共有を表示して、ユーザがアクセスできるようにします。

デフォルト

このコマンドのデフォルト動作は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
グループ webvpn コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。

hidden-shares コマンドの **no** 形式を使用すると、コンフィギュレーションからオプションが削除され、グループ ポリシー属性として非表示共有がディセーブルになります。

例

次に、GroupPolicy2 に関連する WebVPN CIFS 非表示共有を可視にする例を示します。

```
hostname(config)# webvpn
hostname(config-group-policy)#  group-policy GroupPolicy2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# hidden-shares visible
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または WebVPN モードでのグループの WebVPN 属性の設定ができます。
url-list	（グローバル コンフィギュレーション モード）WebVPN ユーザがアクセスする URL のセットを設定します。
url-list	（WebVPN モード）WebVPN サーバおよび URL のリストを特定のユーザまたはグループ ポリシーに適用します。

hold-time

セキュリティ アプライアンスが EIGRP hello パケットでアドバタイズするホールド タイムを指定するには、インターフェイス コンフィギュレーション モードで **hold-time** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	ホールド タイムを秒数で指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

デフォルトの *seconds* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

この値は、セキュリティ アプライアンスによって EIGRP hello パケットでアドバタイズされます。そのインターフェイスの EIGRP ネイバーは、この値を使用してセキュリティ アプライアンスの可用性を判断します。アドバタイズされたホールド タイム中にセキュリティ アプライアンスから hello パケットを受信しなかった場合、EIGRP ネイバーはセキュリティ アプライアンスが使用不可であると見なします。

非常に混雑した大規模ネットワークでは、一部のルータおよびアクセス サーバが、デフォルト ホールド タイム内にネイバーから hello パケットを受信できない可能性があります。この場合、ホールド タイムを増やすこともできます。

ホールド タイムは、少なくとも hello 間隔の 3 倍にすることを推奨します。指定したホールド タイム内にセキュリティ アプライアンスで hello パケットを受信しなかった場合、このネイバーを通過するルートは使用不可であると見なされます。

ホールド タイムを増やすと、ネットワーク全体のルート収束が遅くなります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hello-interval	インターフェイス上で送信される EIGRP hello パケット間の間隔を指定します。

homepage

この WebVPN ユーザまたはグループ ポリシーに対してログイン時に表示される Web ページの URL を指定するには、webvpn モードで **homepage** コマンドを使用します。このモードはグループ ポリシー モードまたはユーザ名モードから開始します。設定済みのホームページ（**homepage none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。ホームページの継承を禁止するには、**homepage none** コマンドを使用します。

homepage {value *url-string* **| none}**

no homepage

構文の説明

none	WebVPN ホームページがないことを指定します。ヌル値を設定して、ホームページを拒否します。ホームページを継承しないようにします。
value *url-string*	ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

デフォルト

デフォルトのホームページはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

グループ ポリシーに関連付けられているユーザのホームページ URL を指定するには、このコマンドで url-string の値を入力します。デフォルト グローバル ポリシーからホームページを継承するには、このコマンドの **no** 形式を使用します。クライアントレス ユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。Linux プラットフォームでは、AnyConnect が現在このコマンドをサポートしていないため、コマンドは無視されます。

例

次に、FirstGroup という名前のグループ ポリシーのホームページとして www.example.com を指定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

host

RADIUS アカウンティングを使用して対話するホストを指定するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **host** コマンドを使用します。このモードにアクセスするには、ポリシー マップ タイプ インスペクションの RADIUS アカウンティング サブモードで **parameters** コマンドを使用します。指定したホストをディセーブルにするには、このコマンドの **no** 形式を使用します。このオプションは、デフォルトで無効です。

host *address* [**key** *secret*]

no host *address* [**key** *secret*]

構文の説明

host	RADIUS アカウンティング メッセージを送信する単一のエンドポイントを指定します。
address	RADIUS アカウンティング メッセージを送信するクライアントまたはサーバの IP アドレス。
key	アカウンティング メッセージの無償コピーを送信するエンドポイントの秘密キーを指定するオプションのキーワード。
secret	メッセージの検証に使用されるアカウンティング メッセージを送信するエンドポイントの共有秘密キー。最大 128 の英数字を使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
radius アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、インスタンスを複数設定できます。

例

次に、RADIUS アカウンティングを使用するホストを指定する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# host 209.165.202.128 key cisco123
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

hostname

セキュリティ アプライアンスのホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。ホスト名は、コマンドライン プロンプトとして表示され、複数のデバイスへのセッションを確立している場合に、コマンドを入力している場所を把握するのに役立ちます。

hostname *name*

no hostname [*name*]

構文の説明

name	ホスト名を最大 63 文字で指定します。ホスト名はアルファベットまたは数字で開始および終了する必要があり、間の文字にはアルファベット、数字、またはハイフンのみを使用する必要があります。

デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	英数字以外の文字（ハイフンを除く）は使用できなくなりました。

使用上のガイドライン

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。

コンテキスト内に任意で設定したホスト名は、コマンドラインには表示されませんが、**banner** コマンドの **$(hostname)** トークンでは使用できます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
hostname(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
banner	ログイン バナー、Message-of-The-Day バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

hsi

H.323 プロトコル インスペクションの HSI グループに HSI を追加するには、HSI グループ コンフィギュレーション モードで **hsi** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi *ip_address*

no hsi *ip_address*

構文の説明

ip_address	追加するホストの IP アドレス。HSI グループごとに最大で 5 つの HSI を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HSI グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション ポリシー マップで HSI を HSI グループに追加する例を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi-group	HSI グループを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsi-group

H.323 プロトコル インスペクション用の HSI グループを定義して、HSI コンフィギュレーション モードを開始するには、パラメータ コンフィギュレーション モードで **hsi-group** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi-group *group_id*

no hsi-group *group_id*

構文の説明

group_id	HSI グループの ID 番号（0 ～ 2147483647）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション ポリシー マップで HSI グループを設定する例を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

html-content-filter

このユーザまたはグループ ポリシーに対して WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、webvpn コンフィギュレーション モードで **html-content-filter** コマンドを使用します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を使用します。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

構文の説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> タグを削除します）。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

デフォルト

フィルタリングは行われません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

すべてのコンテンツ フィルタ（**html-content-filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を引数なしで使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。html コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

例

次に、FirstGroup という名前のグループ ポリシーに対して JAVA と ActiveX、クッキー、およびイメージのフィルタリングを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn（グループ ポリシー、ユーザ名）	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

http

セキュリティ アプライアンス内部の HTTP サーバにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つ以上のホストを削除するには、このコマンドの **no** 形式を使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。

http *ip_address subnet_mask interface_name*

no http

構文の説明

interface_name	ホストが HTTP サーバにアクセスするために通過するセキュリティ アプライアンスのインターフェイスの名前を指定します。
ip_address	HTTP サーバにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバにアクセスできるホストのサブネット マスクを指定します。

デフォルト

HTTP サーバにアクセスできるホストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、IP アドレス 10.10.99.1 とサブネット マスク 255.255.255.255 を持つホストが、外部インターフェイス経由で HTTP サーバにアクセスできるようにする例を示します。

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

次に、任意のホストが、外部インターフェイス経由で HTTP サーバにアクセスできるようにする例を示します。

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザの証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http-comp

特定のグループまたはユーザの WebVPN 接続上で http データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで **http-comp** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

構文の説明

gzip	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

デフォルト

デフォルトでは、圧縮は *gzip* に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

WebVPN 接続の場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで設定された **http-comp** コマンドが上書きされます。

例

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

関連コマンド

コマンド	説明
compression	すべての SVC、WebVPN、IPSec VPN 接続で、圧縮をイネーブルにします。

http-proxy

外部プロキシ サーバを使用して HTTP 要求を処理するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。HTTP プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

http-proxy {*host* [*port*] [**exclude** *url*] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

構文の説明

host	外部 HTTP プロキシ サーバのホスト名または IP アドレス。
pac *pacfile*	1 つ以上のプロキシを指定する JavaScript 関数を含む PAC ファイルを指定します。
password	（任意。*username* を指定した場合に限り使用可能）各 HTTP プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTP 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTP プロキシ サーバによって使用されるポート番号。デフォルト ポートは 80 です。値を指定しなかった場合、セキュリティ アプライアンスはこのポートを使用します。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTP 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTP プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**exclude**、**username**、および **password** のキーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

セキュリティ アプライアンスでサポートされるのは、http-proxy コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての http-proxy コマンドがリストされます。応答に **http-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTP プロキシ サーバの使用を設定する方法を示しています。IP アドレスが 209.165.201.2 のデフォルト ポート（443）を使用。

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 209.165.201.2
hostname(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTP 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
hostname(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、セキュリティ アプライアンスが HTTP 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
hostname(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)
```

次に、exclude オプションの使用例を示します。

```
hostname(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
hostname(config-webvpn)
```

次に、pac オプションを使用する例を示します。

```
hostname(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
https-proxy	外部プロキシ サーバを使用して HTTPS 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

http-proxy（dap）

HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにするには、dap webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。
コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

http-proxy {enable | disable | auto-start}

no http-proxy

構文の説明

auto-start	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルにし、自動的に開始します。
enable/disable	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードで HTTP プロキシをディセーブルにすると、セキュリティ アプライアンスはそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値

を使用すると、属性は DAP レコードには存在しないため、セキュリティ アプライアンスは適用する値を見つけるために、ユーザ名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。

例

次に、Finance という名前のダイナミック アクセス ポリシー レコードに対して HTTP プロキシ ポート フォワーディングをイネーブルにする例を示します。

```
hostname (config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# http-proxy enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

http redirect

セキュリティ アプライアンスによる HTTP 接続の HTTPS へのリダイレクトを指定するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。指定した http redirect コマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。すべての http redirect コマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを引数なしで使用します。

http redirect *interface* [*port*]

no http redirect [*interface*]

構文の説明

interface	セキュリティ アプライアンスで HTTP 要求を HTTPS にリダイレクトする必要があるインターフェイスを識別します。
port	セキュリティ アプライアンスが HTTP 要求をリッスンするポートを識別します。HTTP 要求はリッスン後 HTTPS にリダイレクトされます。デフォルトでは、ポート 80 でリッスンします。

デフォルト

HTTP リダイレクトはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスには、HTTP を許可するアクセス リストが必要です。アクセス リストがない場合、セキュリティ アプライアンスはポート 80 も HTTP 用に設定した他のどのポートもリッスンしません。

例

次に、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する例を示します。

```
hostname(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由するセキュリティ アプライアンスのインターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザの証明書による認証を要求します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server enable

セキュリティ アプライアンスの HTTP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **http server enable** コマンドを使用します。HTTP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server enable [*port*]

no http server enable [*port*]

構文の説明

port	HTTP 接続に使用するポート。範囲は 1 ～ 65535 です。デフォルトのポートは 443 です。

デフォルト

HTTP サーバはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、HTTP サーバをイネーブルにする例を示します。

```
hostname(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由するセキュリティ アプライアンスのインターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザの証明書による認証を要求します。

コマンド	説明
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

https-proxy

外部プロキシ サーバを使用して HTTPS 要求を処理するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モードで **https-proxy** コマンドを使用します。HTTPS プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

構文の説明

host	外部 HTTPS プロキシ サーバのホスト名または IP アドレス。
password	（任意。*username* を指定した場合に限り使用可能）各 HTTPS プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTPS 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTPS プロキシ サーバによって使用されるポート番号。デフォルト ポートは 443 です。値を指定しなかった場合、セキュリティ アプライアンスはこのポートを使用します。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x-y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [**!***x-y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTPS 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTPS プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	**exclude**、**username**、および **password** のキーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

セキュリティ アプライアンスでサポートされるのは、https-proxy コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての https-proxy コマンドがリストされます。応答に **https-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTPS プロキシ サーバの使用を設定する方法を示しています：IP アドレスが 209.165.201.2 のデフォルト ポート（443）を使用。

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 209.165.201.2
hostname(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTPS 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
hostname(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、セキュリティ アプライアンスが HTTPS 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
hostname(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)

hostname(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
hostname(config-webvpn)
```

次に、pac オプションを使用する例を示します。

```
hostname(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
http-proxy	外部プロキシ サーバを使用して HTTP 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

hw-module module password-reset

ハードウェア モジュールのパスワードをデフォルト値「cisco」にリセットするには、特権 EXEC モードで **hw-module module password reset** コマンドを使用します。

hw-module module slot# password-reset

構文の説明

slot#	スロット番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ハードウェア モジュールがアップ状態で、パスワード リセットがサポートされている場合にのみ有効です。AIP SSM でこのコマンドを実行すると、モジュールのリブートが発生します。モジュールは、リブートが完了するまで、オフライン状態になります。これには数分かかる場合があります。**show module** コマンドを実行すると、モジュールの状態をモニタできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。表示される可能性のあるエラー メッセージは、次のとおりです。

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type

The module is slot [n] does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

例

次に、スロット 1 のハードウェア モジュールのパスワードをリセットする例を示します。

```
hostname (config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM ハードウェアをシャットダウンしてリセットします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module recover

TFTP サーバからインテリジェント SSM（AIP SSM など）にリカバリ ソフトウェア イメージをロードしたり、TFTP サーバにアクセスするためのネットワーク設定を行ったりするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。たとえば、SSM で論理イメージをロードできない場合には、このコマンドを使用して SSM を回復する必要があります。このコマンドは、インターフェイスの SSM（4GE SSM など）には使用できません。

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *port_ip_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

構文の説明

1	スロット番号を指定します。これは常に 1 です。
boot	この SSM のリカバリを開始し、**configure** 設定に従ってリカバリ イメージをダウンロードします。ダウンロード後、SSM は新しいイメージからリブートします。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。**configure** キーワードの後にネットワーク パラメータを何も入力しなかった場合、入力を求めるプロンプトが表示されます。
gateway *gateway_ip_address*	（任意）SSM 管理インターフェイスを介して TFTP サーバにアクセスするためのゲートウェイ IP アドレス。
ip *port_ip_address*	（任意）SSM 管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。SSM は元のイメージから起動します。このコマンドは、**hw-module module boot** コマンドを使用してリカバリを開始してから 30 ～ 45 秒以内に入力する必要があります。この期間が経過した後で **stop** コマンドを入力すると、SSM が無応答になるなど、予期しない結果になることがあります。
url *tfp_url*	（任意）TFTP サーバ上のイメージの URL。次の形式で指定します。 **tftp:**//*server*/[*path*/]*filename*
vlan *vlan_id*	（任意）管理インターフェイスの VLAN ID を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SSM がアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ使用可能です。ステート情報については、**show module** コマンドを参照してください。

例

次に、TFTP サーバからイメージをダウンロードするように SSM を設定する例を示します。

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次に、SSM を回復する例を示します。

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reload

インテリジェント SSM ソフトウェア（AIP SSM など）をリロードするには、特権 EXEC モードで **hw-module module reload** コマンドを使用します。このコマンドは、インターフェイスの SSM（4GE SSM など）には使用できません。

hw-module module 1 reload

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SSM ステータスがアップである場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

このコマンドは、ハードウェア リセットも実行する **hw-module module reset** コマンドとは異なります。

例

次に、スロット 1 の SSM をリロードする例を示します。

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。

コマンド	説明
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reset

SSM ハードウェアをシャットダウンしてリセットするには、特権 EXEC モードで **hw-module module reset** コマンドを使用します。

hw-module module 1 reset

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SSM ステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

SSM がアップ状態の場合、**hw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

インテリジェント SSM（AIP SSM など）は、**hw-module module recover** コマンドを使用することで回復できます。SSM が回復状態になっているときに **hw-module module reset** を入力しても、SSM は回復プロセスを中断しません。**hw-module module reset** コマンドによって、SSM のハードウェア リセットが実行され、ハードウェアのリセット後に SSM リカバリが続行されます。SSM がハングした場合は、リカバリ中に SSM をリセットできます。ハードウェア リセットによって、問題が解決することもあります。

このコマンドは、ソフトウェアのリロードのみを行いハードウェア リセットは行わない **hw-module module reload** コマンドとは異なります。

例

次に、アップ状態になっているスロット 1 の SSM をリセットする例を示します。

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

```
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module shutdown

SSM ソフトウェアをシャットダウンするには、特権 EXEC モードで **hw-module module shutdown** コマンドを使用します。

hw-module module 1 shutdown

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSM ソフトウェアをシャットダウンすることによって、コンフィギュレーション データを失うことなく、安全に SSM の電源を切る準備をします。

このコマンドは、SSM ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、スロット 1 の SSM をシャットダウンする例を示します。

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。

コマンド	説明
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
show module	SSM 情報を表示します。

CHAPTER 14

icmp コマンド ～ import webvpn webcontent コマンド

icmp

セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定するには、**icmp** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

構文の説明

deny	条件に合致している場合、アクセスを拒否します。
icmp_type	（任意）ICMP メッセージ タイプ（表 3 を参照）。
if_name	インターフェイス名。
ip_address	ICMP メッセージをインターフェイスに送信しているホストの IP アドレス。
net_mask	*ip_address* に適用されるマスク。
permit	条件に合致している場合、アクセスを許可します。

デフォルト

セキュリティ アプライアンスのデフォルトの動作は、セキュリティ アプライアンス インターフェイス*に向かう*すべての ICMP トラフィックを許可することです。ただし、セキュリティ アプライアンスはデフォルトではブロードキャスト アドレスに送信される ICMP エコー要求に応答しません。また、セキュリティ アプライアンスは宛先が保護されたインターフェイスにある場合、は外部インターフェイスで受信された ICMP メッセージを拒否します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
6.0	このコマンドが導入されました。

使用上のガイドライン

icmp コマンドは、セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックを制御します。ICMP コントロール リストが設定されていない場合、セキュリティ アプライアンスは外部インターフェイスを含め任意のインターフェイスで終了するすべての ICMP トラフィックを受け付けます。ただし、セキュリティ アプライアンスはデフォルトではブロードキャスト アドレスに送信される ICMP エコー要求に応答しません。

セキュリティ アプライアンスは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

icmp deny コマンドはインターフェイスへの ping の実行をディセーブルにし、**icmp permit** コマンドはインターフェイスへの ping の実行をイネーブルにします。ping の実行がディセーブルの場合、セキュリティ アプライアンスはネットワーク上で検出できません。これは、設定可能なプロキシ ping とも呼ばれます。

宛先が保護されたインターフェイスにある場合、**access-list extended** コマンドまたは **access-group** コマンドはセキュリティ アプライアンス*経由で*ルーティングされる ICMP トラフィックに対して使用します。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

インターフェイスの ICMP コントロール リストが設定されている場合、セキュリティ アプライアンスは指定された ICMP トラフィックを照合し、そのインターフェイス上の他のすべての ICMP トラフィックに関して暗黙拒否を適用します。つまり、最初に一致したエントリが許可エントリである場合、ICMP パケットは引き続き処理されます。最初に一致したエントリが拒否エントリであるか、エントリに一致しない場合、セキュリティ アプライアンスによって ICMP パケットは破棄され、syslog メッセージが生成されます。例外は、ICMP コントロール リストが設定されていない場合です。その場合、**permit** ステートメントがあるものと見なされます。

表 3 に、サポートされている ICMP タイプの値を示します。

表 14-1　ICMP タイプおよびリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
8	echo
11	time-exceeded

例

次に、外部インターフェイスですべての ping 要求を拒否し、すべての到達不能メッセージを許可する例を示します。

```
hostname(config)# icmp permit any unreachable outside
```

ICMP トラフィックを拒否するその他のインターフェイスごとに **icmp deny any** *interface* コマンドの入力を続行します。

次に、ホスト 172.16.2.15 またはサブネット 172.22.1.0/16 上のホストに外部インターフェイスへの ping の実行を許可する例を示します。

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

icmp unreachable

セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに到達不能な ICMP メッセージ レート制限を設定するには、**icmp unreachable** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

icmp unreachable rate-limit *rate* **burst-size** *size*

no icmp unreachable rate-limit *rate* **burst-size** *size*

構文の説明

rate-limit *rate*	到達不能メッセージのレート制限を 1 秒あたり 1 ～ 100 メッセージに設定します。デフォルトは、1 秒あたり 1 メッセージです。
burst-size *size*	バースト レートを 1 ～ 10 に設定します。このキーワードは、現在システムで使用されていないため、任意の値を選択できます。

デフォルト

デフォルトのレート制限は、1 秒あたり 1 メッセージです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

到達不能メッセージなどの ICMP メッセージにセキュリティ アプライアンス インターフェイスでの終了を許可する（**icmp** コマンドを参照）場合は、到達不能メッセージのレートを制御できます。

セキュリティ アプライアンスをホップの 1 つとして表示する traceroute がセキュリティ アプライアンスを経由できるようにするには、**set connection decrement-ttl** コマンドとともにこのコマンドが必要です。

例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
set connection decrement-ttl	パケットの存続可能時間の値をデクリメントします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

icmp-object

ICMP タイプのオブジェクト グループを追加するには、ICMP タイプ コンフィギュレーション モードで **icmp-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

icmp-object *icmp_type*

no group-object *icmp_type*

構文の説明

icmp_type	ICMP タイプの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ICMP タイプ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

icmp-object コマンドは、ICMP タイプのオブジェクトを定義するために、**object-group** コマンドとともに使用されます。また、ICMP タイプ コンフィギュレーション モードで使用されます。

ICMP タイプの番号と名前には、次のものがあります。

番号	ICMP タイプ名
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**

番号	ICMP タイプ名
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

例

次に、ICMP タイプ コンフィギュレーション モードで **icmp-object** コマンドを使用する例を示します。

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

id-cert-issuer

システムがこのトラストポイントに関連付けられた CA が発行したピア証明書を受け付けるかどうかを示すには、クリプト CA トラストポイント コンフィギュレーション モードで **id-cert-issuer** コマンドを使用します。トラストポイントに関連付けられた CA が発行した証明書を禁止するには、このコマンドの **no** 形式を使用します。これは、広く使用されているルート CA を表すトラストポイントに便利です。

id-cert-issuer

no id-cert-issuer

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定はイネーブルになっています（アイデンティティ証明書は受け付けられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、広く使用されているルート証明書の下位証明書が発行した証明書に限って受け付けることができます。この機能を許可しないと、セキュリティ アプライアンスはこの発行者によって署名された IKE ピア証明書を拒否します。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、管理者がトラストポイント central の発行者によって署名されたアイデンティティ証明書を受け付ける例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

id-mismatch

過度の DNS ID 不一致のロギングをイネーブルにするには、パラメータ コンフィギュレーション モードで **id-mismatch** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] [**action log**]

構文の説明

count *number*	不一致の最大数。この数を超えると、システム メッセージ ログが送信されます。
duration *seconds*	モニタする期間（秒単位）。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。コマンドがイネーブルで、オプションが指定されていない場合、デフォルトのレートは 3 秒間で 30 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ID 不一致のレートが高い場合、キャッシュ侵害攻撃が発生している可能性があります。このコマンドをイネーブルにすると、このような攻撃をモニタし、警告を発することができます。不一致レートが設定値を超えた場合、システム メッセージ ログを要約したものが印刷されます。**id-mismatch** コマンドを使用すると、システム管理者は通常のイベントベースのシステム メッセージ ログに加え、さらに情報を得ることができます。

例

次に、DNS インスペクション ポリシー マップで ID 不一致をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-mismatch action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

id-randomization

DNS クエリーの DNS 識別子をランダム化するには、パラメータ コンフィギュレーション モードで **id-randomization** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

id-randomization

no id-randomization

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ディセーブルです。DNS クエリーからの DNS 識別子は変更されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ID のランダム化は、キャッシュ侵害攻撃からの保護に役立ちます。

例

次に、DNS インスペクション ポリシー マップで ID のランダム化をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-randomization
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

id-usage（クリプト CA トラスト ポイント）

証明書の登録済み ID を使用できることを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **id-usage** コマンドを使用します。証明書の使用をデフォルト（**ssl-ipsec**）に設定するには、このコマンドの **no** 形式を使用します。

id-usage {ssl-ipsec | code-signer}

no id-usage {ssl-ipsec | code-signer}

構文の説明

code-signer	この証明書で表されるデバイスの ID は、リモート ユーザに提供されるアプレットを検証する際に Java コード署名者として使用されます。
ssl-ipsec	（デフォルト）この証明書で表されるデバイスの ID は、SSL 接続または IPSec-encrypted 接続のサーバ側 ID として使用できます。

デフォルト

id-usage コマンドのデフォルトは **ssl-ipsec** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

リモート アクセス VPN では、配置要件に応じて SSL、IPSec、またはその両方のプロトコルを使用して、ほとんどすべてのネットワーク アプリケーションまたはリソースへのアクセスを許可できます。**id-usage** コマンドを使用すると、証明書で保護されたさまざまなリソースへのアクセスのタイプを指定できます。

CA の ID と、場合によってはデバイスの ID は、CA が発行した証明書に基づいています。クリプト CA トラストポイント モードのすべてのコマンドは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から自身の証明書を取得する方法、および CA によって発行されるユーザ証明書の認証ポリシーを指定する、CA 固有のコンフィギュレーション パラメータを制御します。

id-usage コマンドは、1 つのトラストポイント コンフィギュレーションに 1 回のみ指定できます。code-signer か ssl-ipsec、またはその両方のトラストポイントをイネーブルにするには、コマンドを 1 回のみ使用して、いずれか一方または両方のオプションを指定できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、トラストポイント central をコード署名者の証明書に指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# id-usage code-signer
hostname(config-ca-trustpoint)#
```

次に、トラストポイント general のクリプト CA トラストポイント コンフィギュレーション モードを開始し、トラストポイント general をコード署名者の証明書として、かつ SSL 接続または IPSec 接続のサーバ側 ID として指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 のクリプト CA トラストポイント コンフィギュレーション モードを開始し、トラストポイント checkin1 の使用を SSL 接続または IPSec 接続に制限するようにトラストポイント checkin1 をリセットする例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# no id-usage ssl-ipsec
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
java-trustpoint	指定されたトラストポイントの場所から PKCS12 証明書およびキー関連情報を使用するように WebVPN Java オブジェクト署名機能を設定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書を指定します。
trust-point（トンネル グループ **ipsec** 属性コンフィギュレーション モード）	IKE ピアに送信される証明書を識別する名前を指定します。
validation-policy	ユーザ接続に関連付けられた証明書を検証する条件を指定します。

igmp

インターフェイスでの IGMP 処理を元の状態に戻すには、インターフェイス コンフィギュレーション モードで **igmp** コマンドを使用します。インターフェイスで IGMP 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

igmp

no igmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、選択したインターフェイス上の IGMP 処理をディセーブルにする例を示します。

```
hostname(config-if)# no igmp
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp access-group

インターフェイスからサービスを提供されているサブネット上のホストが参加できるマルチキャスト グループを制御するには、インターフェイス コンフィギュレーション モードで **igmp access-group** コマンドを使用します。インターフェイスでグループをディセーブルにするには、このコマンドの **no** 形式を使用します。

igmp access-group *acl*

no igmp access-group *acl*

構文の説明

acl	IP アクセス リスト名。標準のアクセス リストまたは拡張アクセス リストを指定できます。ただし、拡張アクセス リストを指定した場合は、宛先アドレスのみが照合されるため、送信元には任意のアドレスを指定できます。

デフォルト

すべてのグループがインターフェイスでの参加を許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

例

次に、アクセス リスト 1 でグループへの参加を許可するホストを制限する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp forward interface

すべての IGMP ホスト レポートの転送をイネーブルにし、受信したメッセージを指定されたインターフェイスに残しておくには、インターフェイス コンフィギュレーション モードで **igmp forward interface** コマンドを使用します。転送を削除するには、このコマンドの **no** 形式を使用します。

igmp forward interface *if-name*

no igmp forward interface *if-name*

構文の説明

if-name	インターフェイスの論理名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

入力インターフェイスでこのコマンドを入力します。このコマンドは、スタブ マルチキャスト ルーティングに使用されるため、PIM と同時には設定できません。

例

次に、IGMP ホスト レポートを現在のインターフェイスから指定したインターフェイスに転送する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp join-group

指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **igmp join-group** コマンドを使用します。グループのメンバーシップをキャンセルするには、このコマンドの **no** 形式を使用します。

igmp join-group *group-address*

no igmp join-group *group-address*

構文の説明

group-address	マルチキャスト グループの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドは、マルチキャスト グループのメンバーとなるようにセキュリティ アプライアンス インターフェイスを設定します。**igmp join-group** コマンドを使用すると、セキュリティ アプライアンスは指定したマルチキャスト グループ宛てのマルチキャスト パケット受け付けて転送するようになります。

マルチキャスト グループのメンバーにならずにマルチキャスト トラフィックを転送するようにセキュリティ アプライアンスを設定するには、**igmp static-group** コマンドを使用します。

例

次に、IGMP グループ 255.2.2.2 に参加するように、選択したインターフェイスを設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

関連コマンド

コマンド	説明
igmp static-group	指定したマルチキャスト グループのスタティックに接続されたメンバーになるように、インターフェイスを設定します。

igmp limit

インターフェイス単位で IGMP 状態の数を制限するには、インターフェイス コンフィギュレーション モードで **igmp limit** コマンドを使用します。デフォルトの制限に戻すには、このコマンドの **no** 形式を使用します。

igmp limit *number*

no igmp limit [*number*]

構文の説明

number	インターフェイスで許可されている IGMP 状態の数。有効な値の範囲は、0 ～ 500 です。デフォルト値は 500 です。この値を 0 に設定すると、学習したグループが追加されなくなりますが、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）手動で定義したメンバーシップは引き続き許可されます。

デフォルト

デフォルトは 500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。**igmp max-groups** コマンドに置き換わるものです。

例

次に、インターフェイス上の IGMP 状態の数を 250 に制限する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

関連コマンド

コマンド	説明
igmp	インターフェイス上の IGMP 処理を元の状態に戻します。
igmp join-group	指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定します。
igmp static-group	指定したマルチキャスト グループのスタティックに接続されたメンバーになるように、インターフェイスを設定します。

igmp query-interval

IGMP ホスト クエリー メッセージがインターフェイスによって送信される頻度を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

igmp query-interval *seconds*

no igmp query-interval *seconds*

構文の説明

seconds	IGMP ホスト クエリー メッセージを送信する頻度（秒単位）。有効な値の範囲は、1 ～ 3600 です。デフォルト値は 125 秒です。

デフォルト

デフォルトのクエリー間隔は 125 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

マルチキャスト ルータは、ホスト クエリー メッセージを送信して、インターフェイスにアタッチされているネットワークでどのマルチキャスト グループがメンバーを持っているかを検出します。ホストは、特定のグループのマルチキャスト パケットを受信することを示す IGMP レポート メッセージで応答します。ホスト クエリー メッセージは、アドレスが 224.0.0.1 で、TTL 値が 1 である all-hosts マルチキャスト グループ宛てに送信されます。

LAN の指定ルータが、IGMP ホスト クエリー メッセージを送信する唯一のルータです。

- IGMP バージョン 1 の場合、指定ルータは LAN で稼働するマルチキャスト ルーティング プロトコルに従って選択されます。
- IGMP バージョン 2 の場合、指定ルータはサブネットで最も小さな IP アドレスが指定されたマルチキャスト ルータです。

ルータは、タイムアウト期間（**igmp query-timeout** コマンドで制御）にクエリーを受信しないとクエリアになります。

注意　この値を変更すると、マルチキャスト転送に深刻な影響が及ぶ可能性があります。

例

次に、IGMP クエリー間隔を 120 秒に変更する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

igmp query-max-response-time

IGMP クエリーでアドバタイズされる最大応答時間を指定するには、インターフェイス コンフィギュレーション モードで **igmp query-max-response-time** コマンドを使用します。デフォルトの応答時間に戻すには、このコマンドの **no** 形式を使用します。

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

構文の説明

seconds	IGMP クエリーでアドバタイズされる最大応答時間（秒単位）。有効な値は、1 ～ 25 です。デフォルト値は 10 秒です。

デフォルト

10 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドは、IGMP バージョン 2 または 3 が実行されているときにだけ有効です。

このコマンドは、応答側が IGMP クエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータはグループを削除します。

例

次に、最大クエリー応答時間を 8 秒に変更する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

関連コマンド

コマンド	説明
igmp query-interval	IGMP ホスト クエリー メッセージがインターフェイスによって送信される頻度を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

igmp query-timeout

前のクエリアがクエリーを停止した後でインターフェイスがクエリアを引き継ぐまでのタイムアウト期間を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

構文の説明

seconds	前のクエリアがクエリーを停止した後でルータがクエリアを引き継ぐまでの秒数。有効な値は、60 ～ 300 秒です。デフォルト値は 255 秒です。

デフォルト

デフォルトのクエリー間隔は 255 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、IGMP バージョン 2 または 3 が必要です。

例

次に、最後のクエリーを受信してからインターフェイスのクエリアを引き継ぐまで 200 秒待機するようにルータを設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

関連コマンド

コマンド	説明
igmp query-interval	IGMP ホスト クエリー メッセージがインターフェイスによって送信される頻度を設定します。
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。

igmp static-group

指定したマルチキャスト グループのスタティックに接続されたメンバーになるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **igmp static-group** コマンドを使用します。スタティック グループ エントリを削除するには、このコマンドの **no** 形式を使用します。

igmp static-group *group*

no igmp static-group *group*

構文の説明

group	IP マルチキャスト グループ アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

igmp static-group コマンドで設定された場合、セキュリティ アプライアンス インターフェイスは指定されたグループ自体宛てのマルチキャスト パケットを受け付けず、転送のみを行います。特定のマルチキャスト グループのマルチキャスト パケットを受け付けて転送するようにセキュリティ アプライアンスを設定するには、**igmp join-group** コマンドを使用します。**igmp static-group** コマンドと同じグループ アドレスに対して **igmp join-group** コマンドが設定されている場合、**igmp join-group** コマンドが優先され、グループはローカルに参加したグループのように動作します。

例

次に、選択したインターフェイスをマルチキャスト グループ 239.100.100.101 に追加する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

関連コマンド

コマンド	説明
igmp join-group	指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定します。

igmp version

インターフェイスが使用する IGMP のバージョンを設定するには、インターフェイス コンフィギュレーション モードで **igmp version** コマンドを使用します。バージョンをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

構文の説明

1	IGMP バージョン 1。
2	IGMP バージョン 2。

デフォルト

IGMP バージョン 2。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはインターフェイス コンフィギュレーション モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

サブネット上のすべてのルータが、同じバージョンの IGMP をサポートする必要があります。ホストは任意の IGMP バージョン（1 または 2）を搭載でき、セキュリティ アプライアンスはホストの存在を正しく検出して適切にホストを照会できます。

igmp query-max-response-time や **igmp query-timeout** など一部のコマンドでは、IGMP バージョン 2 が必要です。

例

次に、IGMP バージョン 1 を使用するように、選択したインターフェイスを設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

ignore-ipsec-keyusage

IPsec クライアント証明書でキー使用状況チェックを行わないようにするには、設定 CA トラストポイント コンフィギュレーション モードで **ignore-ipsec-keyusage** コマンドを使用します。キー使用状況チェックを再開するには、このコマンドの **no** 形式を使用します。

ignore-ipsec-keyusage

no ignore-ipsec-keyusage

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Config-ca-trustpoint コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは安全対策として導入されましたが、すぐに廃止されました。今後のリリースでは、キー使用状況チェックの停止が提供されない可能性があることに注意してください。

使用上のガイドライン

このコマンドを使用すると、IPsec リモート クライアント証明書のキー使用状況および拡張キー使用状況の値が検証されなくなります。このコマンドはキー使用状況チェックを無視し、非準拠の配置に便利です。

例

次に、キー使用状況チェックの結果を無視する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)#
hostname(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。

ignore lsa mospf

ルータが LSA Type 6 MOSPF パケットを受信したときには syslog メッセージの送信を行わないようにするには、ルータ コンフィギュレーション モードで **ignore lsa mospf** コマンドを使用します。syslog メッセージの送信を復元するには、このコマンドの **no** 形式を使用します。

ignore lsa mospf

no ignore lsa mospf

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Type 6 MOSPF パケットはサポートされていません。

例

次に、LSA Type 6 MOSPF パケットを無視する例を示します。

```
hostname(config-router)# ignore lsa mospf
```

関連コマンド

コマンド	説明
show running-config router ospf	OSPF ルータ コンフィギュレーションを表示します。

ike-retry-count

SSL による接続試行に戻るまでに、Cisco AnyConnect VPN クライアントが IKE を使用して接続を再試行できる最大数を設定するには、グループ ポリシー webvpn コンフィギュレーション モード、またはユーザ名 webvpn コンフィギュレーション モードで **ike-retry-count** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、再試行の最大数をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ike-retry-count {**none** | *value*}

no ike-retry-count [**none** | *value*]

構文の説明

none	再試行を許可しないことを指定します。
value	初期接続障害の後、Cisco AnyConnect VPN クライアントが接続を再試行できる最大数（1 ～ 10）を指定します。

デフォルト

許可されている再試行のデフォルトの回数は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco AnyConnect VPN クライアントが IKE を使用して接続を試行できる回数を制御するには、**ike-retry-count** コマンドを使用します。IKE を使用して接続に失敗した回数がこのコマンドに指定された再試行数を上回ると、SSL による接続試行に戻ります。この値は、Cisco AnyConnect VPN クライアントに存在する値を上書きします。

（注）　IPSec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** と **ipsec** の両方の引数を設定する必要があります。

例

次に、FirstGroup というグループ ポリシーの IKE 再試行回数を 7 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-count 7
hostname(config-group-webvpn)#
```

次に、ユーザ名 Finance の IKE 再試行回数を 9 に設定する例を示します。

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-count 9
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成または編集します。
ike-retry-timeout	IKE 再試行間の秒数を指定します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
vpn-tunnel-protocol	VPN トンネル タイプ（IPSec、L2TP over IPSec、または WebVPN）を設定します。
webvpn（グループ ポリシー モードまたはユーザ名モード）	グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードを開始します。

ike-retry-timeout

Cisco AnyConnect VPN Client の IKE 再試行の間隔を秒数で設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **ike-retry-timeout** コマンドを使用します。このコマンドをコンフィギュレーションから削除する場合や、タイムアウト値をデフォルト値にリセットする場合は、このコマンドの **no** 形式を使用します。

ike-retry-count *seconds*

no ike-retry-count

構文の説明

seconds	Cisco AnyConnect VPN Client が、最初の接続の失敗後に実行する IKE 再試行の間隔（1 ～ 3600) を秒数で指定します。

デフォルト

デフォルトのタイムアウトは 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco AnyConnect VPN Client の IKE 再試行の間隔（時間の長さ）を制御するには、**ike-retry-timeout** コマンドを使用します。クライアントが、**ike-retry-count** コマンドで指定された数の再試行を行った後で、IKE を使用した接続に失敗した場合は、SSL に戻って接続が試行されます。この値は、Cisco AnyConnect VPN クライアントに存在する値を上書きします。

（注） IPSec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** と **ipsec** の両方の引数を設定する必要があります。

例

次の例では、FirstGroup というグループ ポリシーに対して、IKE 再試行間隔を 77 秒に設定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-timeout 77
hostname(config-group-webvpn)#
```

次の例では、Finance というユーザ名に対して、IKE 再試行回数を 99 回に設定しています。

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-timeout 9
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成または編集します。
ike-retry-count	IKE を使用する Cisco AnyConnect VPN Client が、SSL に戻って接続を試行する前に実行する接続再試行の最大数を指定します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
vpn-tunnel-protocol	VPN トンネル タイプ（IPSec、L2TP over IPSec、または WebVPN）を設定します。
webvpn（グループ ポリシー モードまたはユーザ名モード）	グループ ポリシー webvpn モードまたはユーザ名 webvpn モードに入ります。

im

SIP を経由するインスタント メッセージングをイネーブルにするには、パラメータ コンフィギュレーション モードで **im** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

im

no im

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由するインスタント メッセージングをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# im
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

imap4s

IMAP4S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **imap4s** コマンドを使用します。IMAP4S コマンド モードで入力されたコマンドを削除するには、このコマンドの **no** 形式を使用します。

IMAP4 は、インターネット サーバが電子メールを受信し、保持する際に使用するクライアント/サーバ プロトコルです。ユーザ（または電子メール クライアント）は、電子メールのヘッダーおよび送信者だけを表示して、電子メールをダウンロードするかどうかを判別できます。また、サーバに複数のフォルダまたはメールボックスを作成および操作したり、メッセージを削除したり、メッセージの一部または全体を検索したりできます。IMAP では、電子メールでの作業中、サーバに連続してアクセスする必要があります。IMAP4S を使用すると、SSL 接続で電子メールを受信できます。

imap4s

no imap4s

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、IMAP4S コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
show running-config imap4s	IMAP4S の実行コンフィギュレーションを表示します。

import webvpn customization

カスタマイゼーション オブジェクトをセキュリティ アプライアンスのフラッシュ デバイスにロードするには、特権 EXEC モードで **import webvpn customization** コマンドを入力します。

import webvpn customization *name URL*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大 64 文字です。
URL	XML カスタマイゼーション オブジェクトのソースへのリモート パス。最大 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

import customization コマンドを入力する前に、セキュリティ アプライアンス インターフェイスで WebVPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

カスタマイゼーション オブジェクトをインポートすると、セキュリティ アプライアンスは次のことを行います。

- カスタマイゼーション オブジェクトを URL からセキュリティ アプライアンス ファイル システム disk0:/csco_config/customization に MD5*name* としてコピーします。
- ファイルに対して基本的な XML 構文チェックを実行します。無効な場合、セキュリティ アプライアンスはファイルを削除します。
- index.ini ファイルにレコード MD5*name* が含まれていることをチェックします。含まれていない場合、セキュリティ アプライアンスは MD5*name* をファイルに追加します。
- MD5*name* ファイルを RAMFS /csco_config/customization/ に ramfs *name* としてコピーします。

例

次に、カスタマイゼーション オブジェクト *General.xml* を URL 209.165.201.22/customization からセキュリティ アプライアンスにインポートし、それに *custom1* という名前を付ける例を示します。

```
hostname# import webvpn customization custom1 tftp://209.165.201.22/customization
/General.xml
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

関連コマンド

コマンド	説明
revert webvpn customization	セキュリティ アプライアンスのフラッシュ デバイスから指定されたカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	セキュリティ アプライアンスのフラッシュ デバイスに存在するカスタマイゼーション オブジェクトを一覧表示します。

import webvpn plug-in protocol

セキュリティ アプライアンスのフラッシュ デバイスにプラグインをインストールするには、特権 EXEC モードで **import webvpn plug-in protocol** コマンドを入力します。

import webvpn plug-in protocol *protocol URL*

構文の説明

protocol	• **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://properjavardp.sourceforge.net/ です。 • **ssh、telnet** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://javassh.org/ です。 **注意** **import webvpn plug-in protocol ssh,telnet** *URL* コマンドは、SSH と Telnet の*両方のプラグインをインストールします。*SSH 用と Telnet 用にこのコマンドをそれぞれ入力*しないでください。***ssh,telnet** ストリングを入力する場合は、両者の間にスペースは挿入*しません。*これらの要件から逸脱する **import webvpn plug-in protocol** コマンドを削除するには、**revert webvpn plug-in protocol** コマンドを使用します。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://www.tightvnc.com/ です。
URL	プラグインのソースへのリモート パス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

プラグインをインストールする前に、次のことを行います。

- セキュリティ アプライアンスのインターフェイス上でクライアントレス SSL VPN（「webvpn」）がイネーブルになっていることを確認します。これを行うには、**show running-config** コマンドを入力します。
- ローカル TFTP サーバ（たとえば、ホスト名が「local_tftp_server」のサーバ）で一時ディレクトリを「plugins」という名前で作成し、プラグインをシスコの Web サイトから「plugins」ディレクトリにダウンロードします。TFTP サーバのホスト名またはアドレスを入力し、必要なプラグインへのパスを **import webvpn plug-in protocol** コマンドの URL フィールドに入力します。

プラグインをインポートすると、セキュリティ アプライアンスは次のことを行います。

- *URL* に指定されている jar ファイルを解凍します。
- そのファイルをセキュリティ アプライアンス ファイル システムの `csco-config/97/plugin` ディレクトリに書き込みます。
- ASDM の URL 属性の横にあるドロップダウン メニューに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、ポータル ページの Address フィールドの横にあるドロップダウン メニューにメイン メニュー オプションとオプションを追加します。表 14-2 に、ポータル ページのメイン メニューと Address フィールドに加えられた変更を示します。

表 14-2　クライアントレス SSL VPN ポータル ページへのプラグインの影響

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
rdp	ターミナル サーバ	rdp://
ssh、telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

セキュリティ アプライアンスは、**import webvpn plug-in protocol** コマンドをコンフィギュレーションに保持しません。その代わりに、csco-config/97/plugin ディレクトリの内容を自動的にロードします。セカンダリ セキュリティ アプライアンスは、プライマリ セキュリティ アプライアンスからプラグインを取得します。

クライアントレス SSL VPN セッションでユーザがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ ペインが表示されます。ドロップダウン メニューに表示されたプロトコルをユーザが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注） SSH クライアントは、SSH バージョン 1.0 のみをサポートします。

Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、セキュリティ アプライアンスではなくステータスをレポートします。

import webvpn plug-in protocol コマンドを個別に削除し、プロトコルのサポートをディセーブルにするには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次のコマンドでは、RDP のクライアントレス SSL VPN サポートを追加しています。

```
hostname# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

次のコマンドでは、SSH および Telnet のクライアントレス SSL VPN サポートを追加しています。

```
hostname# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar

Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

次のコマンドでは、VNC のクライアントレス SSL VPN サポートを追加しています。

```
hostname# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar

Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
hostname#
```

関連コマンド

コマンド	説明
revert webvpn plug-in protocol	セキュリティ アプライアンスのフラッシュ デバイスから指定されたプラグインを削除します。
show import webvpn plug-in	セキュリティ アプライアンスのフラッシュ デバイスに存在するプラグインのリストを示します。

import webvpn translation-table

リモート ユーザが SSL VPN 接続を確立するときに表示される言語を変換するために使用される変換テーブルをインポートするには、特権 EXEC モードから **import webvpn translation-table** コマンドを使用します。

import webvpn translation-table *translation_domain* **language** *language url*

構文の説明

language	変換テーブルの言語を指定します。*language* の値は、ブラウザの言語オプションの表現に従って入力します。
translation_domain	リモート ユーザに表示される機能エリアと関連するメッセージ。使用上のガイドラインのセクションに、使用可能な変換ドメインがリストされています。
url	カスタマイゼーション オブジェクトの作成に使用される XML ファイルの URL を指定します。

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

リモート ユーザに表示される各機能エリアとそのメッセージには独自の変換ドメインがあります。この変換ドメインは *translation_domain* 引数で指定します。次の表に、変換ドメインおよび、変換される機能領域を示します。

表 14-3　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。

変換ドメイン	変換される機能エリア
banners	リモート ユーザに表示されるバナーと、VPN アクセスが拒否されたときのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。

変換テンプレートは変換テーブルと同じ形式の XML ファイルですが、変換内容はすべて空です。セキュリティ アプライアンスのソフトウェア イメージ パッケージには、標準機能の一部として各ドメイン用のテンプレートが含まれています。プラグインのテンプレートはプラグインに付属しており、独自の変換ドメインを定義します。クライアントレス ユーザのログインおよびログアウト ページ、ポータル ページ、および URL ブックマークはカスタマイズが可能なため、セキュリティ アプライアンスは **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

export webvpn translation-table コマンドを使用して変換ドメインのテンプレートをダウンロードし、メッセージに変更を加え、**import webvpn translation-table** コマンドを使用してオブジェクトを作成します。**show import webvpn translation-table** コマンドを使用して、使用可能なオブジェクトを表示できます。

ブラウザの言語オプションの表現に従って *language* を指定してください。たとえば、Microsoft Internet Explorer は中国語に短縮形 ***zh*** を使用します。セキュリティ アプライアンスにインポートする変換テーブルも、*zh* という名前にする必要があります。

カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する変換テーブルを識別し、グループ ポリシーまたはユーザのカスタマイズを指定するまで、AnyConnect 変換ドメインを除いて、変換テーブルは機能せず、メッセージは変換されません。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント ユーザに表示されます。詳細については、**import webvpn customization** コマンドを参照してください。

例

次に、AnyConnect クライアント ユーザ インターフェイスに影響を与える変換ドメインの変換テーブルをインポートし、変換テーブルが中国語用のものであることを指定する例を示します。**show import webvpn translation-table** コマンドは、新規オブジェクトを表示します。

```
hostname# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
```

```
VNC-plugin

Translation Tables:
zh AnyConnect
```

関連コマンド

コマンド	説明
export webvpn translation-table	変換テーブルをエクスポートします。
import webvpn customization	変換テーブルを参照するカスタマイゼーション オブジェクトをインポートします。
revert	フラッシュから変換テーブルを削除します。
show import webvpn translation-table	使用可能な変換テーブル テンプレートおよび変換テーブルを表示します。

import webvpn url-list

セキュリティ アプライアンスのフラッシュ デバイス上に URL リストをロードするには、特権 EXEC モードで **import webvpn url-list** コマンドを使用します。

import webvpn url-list *name URL*

構文の説明

name	URL リストを識別する名前。最大 64 文字です。
URL	URL リストのソースへのリモート パス。最大 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
(8.0(2)	このコマンドが導入されました。

使用上のガイドライン

import url-list コマンドを入力する前に、セキュリティ アプライアンス インターフェイスで WebVPN がイネーブルになっていることを確認します。そのためには、**show running-config** コマンドを入力します。

URL リストをインポートすると、セキュリティ アプライアンスは次のことを行います。

- URL リストを URL からセキュリティ アプライアンス ファイル システム disk0:/csco_config/url-lists に *name on flash* = base 64*name* としてコピーします。
- ファイルに対して基本的な XML 構文チェックを実行します。無効な場合、セキュリティ アプライアンスはファイルを削除します。
- index.ini ファイルにレコード base 64*name* が含まれていることをチェックします。含まれていない場合、セキュリティ アプライアンスは base 64*name* をファイルに追加します。
- *name* ファイルを RAMFS /csco_config/url-lists/ に ramfs name = *name* としてコピーします。

例

次に、*NewList.xml* という URL リストを URL 209.165.201.22/url-lists からセキュリティ アプライアンスにインポートし、それに *ABCList* という名前を付ける例を示します。

```
hostname# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

関連コマンド

コマンド	説明
revert webvpn url-list	セキュリティ アプライアンスのフラッシュ デバイスから指定された URL リストを削除します。
show import webvpn url-list	セキュリティ アプライアンスのフラッシュ デバイスに存在する URL リストを一覧表示します。

import webvpn webcontent

リモートのクライアントレス SSL VPN ユーザに表示されるコンテンツをフラッシュ メモリにインポートするには、特権 EXEC モードから **import webvpn webcontent** コマンドを使用します。

import webvpn webcontent <*destination url*> <*source url*>

構文の説明

<*source url*>	コンテンツがあるセキュリティ アプライアンスのフラッシュ メモリの URL。最大 64 文字です。
<*destination url*>	エクスポート先の URL。最大 255 文字です。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

webcontent オプションでインポートされるコンテンツは、リモートのクライアントレス ユーザに表示されます。この中には、クライアントレス ポータルに表示されるヘルプ コンテンツや、ユーザ画面をカスタマイズするカスタマイゼーション オブジェクトで使用されるロゴなどがあります。

パス /+CSCOE+/ で URL にインポートされるコンテンツは、認可されたユーザにのみ表示されます。

パス /+CSCOU+/ で URL にインポートされるコンテンツは、不正なユーザと認可されたユーザの両方に表示されます。

たとえば、/+CSCOU+/logo.gif としてインポートした企業ロゴを、ポータル カスタマイゼーション オブジェクトに使用し、ログイン ページおよびポータル ページに表示できます。/+CSCOE+/logo.gif としてインポートした同じ logo.gif ファイルは、正常にログインしたリモート ユーザにのみ表示されます。

さまざまなアプリケーション画面に表示されるヘルプ コンテンツは、特定の URL にインポートする必要があります。表 14-4 に、標準のクライアントレス アプリケーション用に表示されるヘルプ コンテンツの URL および画面エリアを示します。

表 14-4　標準のクライアントレス アプリケーション

URL	クライアントレス画面エリア
/+CSCOE+/help/<*language*>/app-access-hlp.inc	アプリケーション アクセス
/+CSCOE+/help/<*language*>/file-access-hlp.inc	ブラウズ ネットワーク
/+CSCOE+/help/<*language*>/net_access_hlp.html	AnyConnect クライアント
/+CSCOE+/help/<*language*>/web-access-help.inc	Web アクセス

表 14-5 に、任意のプラグイン クライアントレス アプリケーション用に表示されるヘルプ コンテンツの URL および画面エリアを示します。

表 14-5　プラグイン クライアントレス アプリケーション

URL	クライアントレス画面エリア
/+CSCOE+/help/<*language*>/ica-hlp.inc	MetaFrame アクセス
/+CSCOE+/help/<*language*>/rdp-hlp.inc	ターミナル サーバ
/+CSCOE+/help/<*language*>/ssh,telnet-hlp.inc	Telnet/SSH サーバ
/+CSCOE+/help/<*language*>/vnc-hlp.inc	VNC コネクション

URL パスの <*language*> は、ヘルプ コンテンツ用に指定した言語の短縮形です。セキュリティ アプライアンスは、ファイルを指定された言語に実際に変換するわけではなく、ファイルに言語の短縮形のラベルを付けます。

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の tftp サーバからフラッシュ メモリ内の Application Access ヘルプ コンテンツを保管する URL にインポートする例を示します。URL には英語の省略形 *en* が含まれています。

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
hostname#
```

例

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の tftp サーバからフラッシュ メモリ内の Application Access ヘルプ コンテンツを保管する URL にインポートする例を示します。URL には英語の省略形 *en* が含まれています。

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
hostname#
```

関連コマンド

コマンド	説明
export webvpn webcontent	クライアントレス SSL VPN ユーザ向けに以前にインポートしたコンテンツをエクスポートします。
revert webvpn webcontent	コンテンツをフラッシュ メモリから削除します。
show import webvpn webcontent	インポートされたコンテンツに関する情報を表示します。

CHAPTER 15

inspect ctiqbe コマンド～ inspect xdmcp コマンド

inspect ctiqbe

CTIQBE プロトコル インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect ctiqbe

no inspect ctiqbe

デフォルト

デフォルトでは、このコマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは 7.0 で追加されました。既存の **fixup** コマンドが廃止され、代わりにこのコマンドが追加されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートしている CTIQBE プロトコル インスペクションをイネーブルにします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、セキュリティ アプライアンス を越えてコール セットアップを行えるようになります。

Telephony Application Programming Interface（TAPI）および Java Telephony Application Programming Interface（JTAPI）は、多数の Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、Cisco TAPI Service Provider（TSP）によって Cisco CallManager と通信するために使用されます。

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションでは、**alias** コマンドを使用したコンフィギュレーションはサポートしていません。
- CTIQBE コールのステートフル フェールオーバーはサポートされて*いません*。
- **debug ctiqbe** コマンドを使用すると、メッセージ送信が遅延することがあり、これによってリアルタイム環境のパフォーマンスに影響が出る可能性があります。このデバッグまたはログをイネーブルにし、セキュリティ アプライアンス を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。
- CTIQBE アプリケーション インスペクションでは、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートして*いません*。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が、セキュリティ アプライアンスのそれぞれ異なるインターフェイスに接続された別々の Cisco CallManager に登録されている場合、これら 2 つの電話機間のコールが失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと**同じポート**にスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect ctiqbe** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect ctiqbe** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect ctiqbe** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、CTIQBE インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（2748）上の CTIQBE トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
show conn	さまざまな接続タイプの接続状態を表示します。

コマンド	説明
show ctiqbe	セキュリティ アプライアンスを通じて確立された CTIQBE セッションに関する情報を表示します。CTIQBE インスペクション エンジンによって割り当てられたメディア接続に関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect dcerpc

エンドポイントマッパー宛ての DCERPC トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect dcerpc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

構文の説明

map_name	（任意）DCERPC マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect dcerpc コマンドは、DCERPC プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc_map

hostname(config)# service-policy global-policy global
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
timeout pinhole	DCERPC ピンホールのタイムアウトを設定して、グローバル システムのピンホール タイムアウトを上書きします。

inspect dns

DNS インスペクションをイネーブルにしたり（ディセーブルになっている場合）、DNS インスペクション パラメータを設定したりするには、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。DNS インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect dns [*map_name*]

no inspect dns [*map_name*]

構文の説明

map_name	（任意）DNS マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。
7.2(1)	このコマンドは、DNS インスペクションの追加パラメータを設定できるように変更されました。

使用上のガイドライン

DNS ガードは、セキュリティ アプライアンスによって DNS 応答が転送されるとすぐに、DNS クエリーに関連付けられている DNS セッションを切断します。また、DNS ガードはメッセージ交換をモニタして、DNS 応答の ID が DNS クエリーの ID と必ず一致するようにします。

DNS インスペクションがイネーブルになっている場合（デフォルト）、セキュリティ アプライアンスは次の追加タスクを実行します。

- **alias**、**static**、および **nat** コマンドを使用して設定されているコンフィギュレーションに基づいて、DNS レコードを変換します（DNS リライト）。変換は、DNS 応答の A レコードにのみ適用されます。そのため、PTR レコードを必要とする逆ルックアップは、DNS リライトの影響を受けません。

（注） 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。

- 最大 DNS メッセージ長を指定します（デフォルトは 512 バイト、最大長は 65535 バイト）。パケット長が設定されている最大長よりも小さいことを検証するために、必要に応じて再構築が実行されます。最大長を超えた場合、パケットはドロップされます。
- ドメイン名の長さを 255 バイトに制限し、ラベルの長さを 63 バイトに制限します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの機能

DNS インスペクションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部のネットワーク上のクライアントが、外部インターフェイス上の DNS サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルである場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、*DNS 応答*のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

DNS インスペクションがイネーブルのままである間、**alias**、**static**、または **nat** コマンドを使用して DNS リライトを設定できます。これらのコマンドの構文および機能の詳細については、該当するコマンド ページを参照してください。

例

次に、DNS メッセージの最大長を設定する例を示します。

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug dns	DNS のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect esmtp

SMTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードは、ポリシー マップ コンフィギュレーション モードからアクセス可能です。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

構文の説明

map_name	（任意）ESMTP マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ESMTP アプリケーション インスペクションを使用すると、セキュリティ アプライアンスを通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張機能であり、ほとんどの点で SMTP と類似しています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

inspect esmtp コマンドには、以前 **fixup smtp** コマンドで提供されていた機能が含まれており、さらに一部の拡張 SMTP コマンドに対するサポートも追加されています。拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）に対するサポートとあわせて、セキュリティ アプライアンスでは合計で 15 個の SMTP コマンドがサポートされています。

ATRN、ONEX、VERB、CHUNKING などのその他の拡張 SMTP コマンドおよびプライベート拡張はサポートされていません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

inspect esmtp コマンドは、サーバ SMTP バナーの「2」、「0」、「0」以外の文字をアスタリスクに変更します。Carriage Return（CR; 復帰）、および Linefeed（LF; 改行）は無視されます。

SMTP インスペクションがイネーブルの場合、次のルールが遵守されていないと、インタラクティブ SMTP に使用されている Telnet セッションは有効なコマンドを待機し、ファイアウォール esmtp ステート マシンはセッションのための正しい状態を保持します。このルールとは、SMTP コマンドは 4 文字以上である必要がある、SMTP コマンドは復帰と改行で終了している必要がある、および SMTP コマンドは次の返信を発行する前に応答を待機する必要がある、というものです。

SMTP サーバは数値の応答コードと人が読めるオプションのストリングを使用してクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL from コマンドまたは RCPT to コマンドに対するパラメータとして PIPE シグニチャが見つかった場合、セッションは閉じられます。ユーザが設定することはできません。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバはクライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリーム編集
- コマンド パイプライン

例

次の例に示すように、SMTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（25）上の SMTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

すべてのインターフェイスに対して SMTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug esmtp	SMTP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SMTP を含む各種接続タイプの接続状態を表示します。

inspect ftp

ポートを FTP インスペクション用に設定したり、拡張インスペクションをイネーブルにしたりするには、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

構文の説明

map_name	FTP マップの名前。
strict	（任意）FTP トラフィックの拡張インスペクションをイネーブルにして、RFC 標準への準拠を強制します。

注意 FTP を上位のポートに移動する場合には注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に対して開始されるすべての接続で、データ ペイロードが FTP コマンドとして解釈されます。

デフォルト

セキュリティ アプライアンスは、デフォルトではポート 21 で FTP をリッスンします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続を準備します。
- **ftp** コマンド応答シーケンスを追跡します。
- 監査証跡の生成
- 埋め込み IP アドレスの NAT を実行します。

（注）　バナーを除いて、**inspect ftp** では FTP コマンドまたは応答をセグメント化する FTP サーバはサポートしていません。

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト作成のイベントに応答してチャネルが割り当てられますが、事前のネゴシエーションが必要です。ポートは、PORT または PASV コマンドを使用してネゴシエートされます。

（注）　FTP コントロール接続のポートだけを指定し、データ接続のポートは指定しないでください。セキュリティ アプライアンスのステートフル インスペクション エンジンは、必要に応じてダイナミックにデータ接続を準備します。

（注）　**no inspect ftp** コマンドを使用して、FTP インスペクション エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

strict オプションの使用方法

strict オプションを使用すると、Web ブラウザは FTP 要求で組み込みコマンドを送信できなくなります。個々の **ftp** コマンドは、新しいコマンドが許可される前に承認される必要があります。組み込みコマンドを送信する接続は、ドロップされます。**strict** オプションを使用すると、FTP サーバは 227 コマンドしか生成できなくなり、FTP クライアントは PORT コマンドしか生成できなくなります。227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

すべてのインターフェイスに対してストリクト FTP アプリケーション インスペクションをイネーブルにするには、**interface** コマンドの代わりに **global** パラメータを使用します。

注意　**strict** オプションを使用すると、RFC 標準に準拠していない FTP クライアントは切断されることがあります。

strict オプションがイネーブルの場合、次の異常なアクティビティに関して、各 **ftp** コマンドと応答シーケンスが追跡されます。

- 切り捨てされたコマンド : PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド : **ftp** コマンドが、RFC で要求されているとおりに <CR><LF> 文字で終了しているかどうかがチェックされます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ : これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- コマンド スプーフィング : PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング : PASV 応答コマンド（227）は、常にサーバから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2.」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集

- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- セキュリティ アプライアンスは、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。このデフォルト動作を上書きするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

（注） セキュリティ アプライアンスの通過を許可しない特定の FTP コマンドを識別するには、FTP マップを識別し **request-command deny** コマンドを使用します。詳細については、**ftp-map** および **request-command deny** コマンドのページを参照してください。

FTP ログ メッセージ

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 取得またはアップロードされたファイルごとに監査レコード 302002 が生成されます。
- **ftp** コマンドが RETR または STOR であるかどうかがチェックされ、取得コマンドおよび格納コマンドがログに記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。

NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

例

ユーザ名とパスワードを送信する前に、すべての FTP ユーザに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
hostname(config-pmap-p)# exit
hostname(config-pmap)# exit
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
hostname(config-cmap)# exit
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy ftp-policy interface inside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
mask-syst-reply	FTP サーバ応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect gtp

GTP インスペクションをイネーブルまたはディセーブルにしたり、GTP トラフィックまたはトンネルを制御するための GTP マップを定義したりするには、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

（注） GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがない状態でセキュリティ アプライアンスで **inspect gtp** コマンドを入力すると、セキュリティ アプライアンスによってエラー メッセージが表示されます。

構文の説明

map_name	（任意）GTP マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

GTP は GPRS のトンネリング プロトコルであり、ワイヤレス ネットワークを介したセキュアなアクセスの提供に役立ちます。GPRS は、既存の GSM ネットワークとの統合を目的としたデータ ネットワーク アーキテクチャです。企業ネットワークおよびインターネットに対する連続したパケットスイッチド データ サービスをモバイル加入者に提供します。GTP の概要については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Applying Application Layer Protocol Inspection」の章を参照してください。

GTP のパラメータの定義に使用する特定のマップを識別するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードを開始して、特定のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**drop**、**rate-limit** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントを**ログに記録**するかどうかも指定できます。

GTP マップを定義した後、**inspect gtp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

GTP の既知のポートは次のとおりです。

- 3386
- 2123

次の機能は 7.0 ではサポートされていません。

- NAT、PAT、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、および 2152 以外のポート
- トンネル IP パケットとその内容の検証

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect gtp** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect gtp** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、アクセス リストを使用して GTP トラフィックを識別し、GTP マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

（注） この例では、デフォルト値で GTP インスペクションをイネーブルにします。デフォルト値を変更するには、**gtp-map** コマンドのページと、GTP マップ コンフィギュレーション モードで入力する各コマンドのコマンド ページを参照してください。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show service-policy inspect gtp	**inspect gtp** ポリシーのステータスおよび統計情報を表示します。

inspect h323

H.323 アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect h323 {**h225** | **ras**} [*map_name*]

no inspect h323 {**h225** | **ras**} [*map_name*]

構文の説明

h225	H.225 シグナリング インスペクションをイネーブルにします。
map_name	（任意）H.323 マップの名前。
ras	RAS インスペクションをイネーブルにします。

デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718 ～ 1719

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager や VocalTec Gatekeeper などの H.323 に準拠したアプリケーションに対するサポートを提供します。H.323 は International Telecommunication Union（ITU; 国際電気通信連合）で定義されている、LAN を介したマルチメディア会議用のプロトコル スイートです。セキュリティ アプライアンスは、One Call Signaling Channel 上の Multiple Calls の H.323 v3 機能など、バージョン 4 までの H.323 をサポートしています。

H.323 インスペクションをイネーブルにした場合、セキュリティ アプライアンス は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、セキュリティ アプライアンス でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、セキュリティ アプライアンス では ASN.1 デコーダを使用して H.323 メッセージを復号化します。

- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 のプロトコル コレクションでは、あわせて最大 2 つの TCP 接続と 4 ～ 6 つの UDP 接続を使用できます。FastStart では 1 つの TCP 接続だけを使用し、RAS では登録、許可、およびステータス用に単一の UDP 接続を使用します。

H.323 クライアントは最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コール設定を要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.245 接続は、コール ネゴシエーションとメディア チャネル設定に使用されます。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末で FastStart を使用していない場合、セキュリティ アプライアンスは H.225 メッセージのインスペクションに基づいて H.245 接続をダイナミックに割り当てます。

（注）　RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。Real-Time Transport Protocol（RTP）はネゴシエートされたポート番号を使用し、RTP Control Protocol（RTCP）はすぐ次の上位ポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出に使用される UDP ポート
- 1719：RAS およびゲートキーパー検出に使用される UDP ポート
- 1720：TCP 制御ポート

ゲートキーパーからの ACF メッセージがセキュリティ アプライアンスを通過する場合は、H.225 接続用のピンホールが開かれます。H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーが使用されると、セキュリティ アプライアンスは ACF メッセージのインスペクションに基づいて H.225 接続を開きます。セキュリティ アプライアンスで ACF メッセージを確認できない場合は、H.225 コール シグナリング用に既知の H.323 ポート 1720 のアクセス リストを開くことが必要になる場合があります。

セキュリティ アプライアンスは H.225 メッセージを検査した後、H.245 チャネルをダイナミックに割り当てて、同様にフィックスアップする H.245 チャネルに接続します。これは、セキュリティ アプライアンスを通過した H.245 メッセージはすべて、H.245 アプリケーション インスペクションを通過し、埋め込み IP アドレスの NAT が実行され、ネゴシエートされたメディア チャネルが開かれることを意味します。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは必ずしも H.225/H.245 メッセージと同じ TCP パケットで送信される必要はないため、セキュリティ アプライアンスではメッセージを正しく処理およびデコードするために TPKT 長を保持しておく必要があります。セキュリティ アプライアンスは接続ごとにデータ構造を保持し、そのデータ構造に次に想定されるメッセージの TPKT 長が格納されます。

セキュリティ アプライアンスで任意の IP アドレスの NAT を実行する必要がある場合は、チェックサム、User-User Information Element（UUIE）長、および TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンスはその TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの新しい TPKT を付加します。

（注）　セキュリティ アプライアンスは、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

パケットが H.323 インスペクションを通過する各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドを使用して設定した H.323 タイムアウト値でタイムアウトします。

制限事項

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション インスペクションは、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録されているときに、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイにコールを発信しようとすると、接続は確立されるが音声が双方向で聞こえないという現象が確認されています。この問題は、セキュリティ アプライアンス の問題ではありません。
- ネットワーク スタティックを設定する場合、そのネットワーク スタティックがサードパーティのネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect h323** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect h323** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、H.323 インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1720）上の H.323 トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

すべてのインターフェイスに対して H.323 インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
show h225	セキュリティ アプライアンスで確立されている H.225 セッションの情報を表示します。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout {**h225** | **h323**}	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

inspect http

HTTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect http** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect http [*map_name*]

no inspect http [*map_name*]

構文の説明

map_name	（任意）HTTP マップの名前。

デフォルト

HTTP のデフォルト ポートは 80 です。

拡張 HTTP インスペクションは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect http コマンドは、HTTP トラフィックに関連付けられている可能性のある特定の攻撃およびその他の脅威を防ぎます。HTTP インスペクションは、次のようないくつかの機能を実行します。

- 拡張 HTTP インスペクション
- N2H2 または Websense を使用する URL のスクリーニング
- Java と ActiveX のフィルタリング

後の 2 つの機能は、**filter** コマンドとともに設定します。

拡張 HTTP インスペクションでは、HTTP メッセージが RFC 2616 に準拠していること、RFC で規定されている方式またはサポートされている拡張方式を使用していること、および他のさまざまな基準に適合していることを検証します。多くの場合、これらの基準と基準を満たしていない場合のシステムの応答を設定できます。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などの異なるコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

HTTP メッセージに適用できる基準は、次のとおりです。

- 設定可能リストに挙げられている方式が含まれていない。

- 特定の転送エンコーディング方式またはアプリケーション タイプ。
- HTTP トランザクションが RFC 仕様に従っている。
- メッセージ本文のサイズが設定可能な限度内である。
- 要求メッセージおよび応答メッセージのヘッダー サイズが設定可能な限度内である。
- URI 長が設定可能な限度内である。
- メッセージ本文の content-type がヘッダーと一致している。
- 応答メッセージの content-type が要求メッセージの *accept-type* フィールドと一致している。
- メッセージの content-type が事前定義済みの内部リストに含まれている。
- メッセージが HTTP RFC 形式の基準を満たしている。
- 選択したサポート対象アプリケーションの有無。
- 選択したエンコーディング タイプの有無。

（注） 基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などの異なるコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

拡張 HTTP インスペクションをイネーブルにするには、**inspect http** *http-map* コマンドを入力します。このコマンドで HTTP トラフィックに適用されるルールは、特定の HTTP マップで定義します。この HTTP マップを設定するには、**http-map** コマンドおよび HTTP マップ コンフィギュレーション モード コマンドを入力します。

（注） HTTP マップで HTTP インスペクションをイネーブルにした場合は、リセットおよびログ アクションを伴う厳格な HTTP インスペクションがデフォルトでイネーブルになります。インスペクションの失敗に対して実行するアクションは変更できますが、HTTP マップがイネーブルになっているかぎり、厳格なインスペクションはディセーブルにできません。

例

次に、HTTP トラフィックを識別し、HTTP マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、セキュリティ アプライアンスは次のコンテンツを含むトラフィックを検出したときに、接続をリセットして Syslog エントリを作成します。

- 100 バイト未満または 2000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	HTTP アプリケーション インスペクションに関する詳細情報を表示します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

inspect icmp

ICMP インスペクション エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp

no inspect icmp

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ICMP インスペクション エンジンを使用すると、TCP や UDP トラフィックのように ICMP トラフィックを検査できます。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP によるセキュリティ アプライアンスの通過を禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンにより、それぞれの要求に対して 1 つの応答しか返されなくなり、正確なシーケンス番号が設定されるようになります。

ICMP インスペクションがディセーブルの場合（デフォルト設定）、セキュリティの低いインターフェイスからセキュリティの高いインターフェイスへの ICMP エコー応答メッセージは、ICMP エコー要求への応答であっても拒否されます。

例

次の例に示すように、ICMP アプリケーション インスペクション エンジンをイネーブルにします。この例では、ICMP プロトコル ID（IPv4 の場合は 1、IPv6 の場合は 58）を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect icmp error

ICMP エラー メッセージに対してアプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect icmp error** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp error

no inspect icmp error

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

スタティック /NAT コンフィギュレーションに基づいて、ICMP エラー メッセージを送信する中間ホップの xlate を作成するには、**inspect icmp error** コマンドを使用します。デフォルトでは、セキュリティ アプライアンスでは中間ホップの IP アドレスは表示されません。ただし、**inspect icmp error** コマンドを使用すると、中間ホップの IP アドレスが表示されるようになります。セキュリティ アプライアンスは、変換後の IP アドレスでパケットを上書きします。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェアでは、パス MTU ディスカバリまたはホップバイホップ ディスカバリに関する ICMP エラー メッセージの生成時に、出力インターフェイス アドレスを送信元アドレスとして使用します。**inspect icmp error** コマンドを使用して ICMP エラー メッセージのアプリケーション インスペクションをイネーブルにすると、NAT もまたこの送信元アドレスに単独で適用されます。

イネーブルになっている場合、ICMP エラー インスペクション エンジンによって次のように ICMP パケットが変更されます。

- IP ヘッダーで、NAT IP が Client IP（宛先アドレスおよび中間ホップ アドレス）に変更され、IP チェックサムが変更されます。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットの NAT IP が Client IP に変更されます。
  - 元のパケットの NAT ポートが Client Port に変更されます。
  - 元のパケットの IP チェックサムを再計算する。

ICMP エラー インスペクションがイネーブルかどうかに関係なく、ICMP エラー メッセージが取得されると、ICMP ペイロードがスキャンされ、元のパケットから 5 つのタプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート、および IP プロトコル）が取得されます。クライアントの元のアドレスを確認し、特定の 5 つのタプルに関連付けられている既存のセッションを検索するために、取得した 5 つのタプルを使用してルックアップが実行されます。セッションが見つからなかった場合、ICMP エラー メッセージはドロップされます。

例

次の例に示すように、ICMP エラー アプリケーション インスペクション エンジンをイネーブルにします。この例では、ICMP プロトコル ID（IPv4 の場合は 1、IPv6 の場合は 58）を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP エラー インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect ils

ILS アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect ils** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ils

no inspect ils

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品に対する NAT のサポートを提供します。

セキュリティ アプライアンス は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、Port Address Translation（PAT; ポート アドレス交換）はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント / サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 参照要求および応答はサポートされない。
- 複数のディレクトリ内のユーザは統合されない。
- 1 人のユーザが複数のディレクトリで複数の ID を持つ場合、NAT はそのユーザを認識できない。

（注）　H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP **timeout** コマンドで指定された間隔が経過すると、TCP 接続は切断されます。デフォルトで、この間隔は 60 分に設定されています。

例

次の例に示すように、ILS インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

すべてのインターフェイスに対して ILS インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug ils	ILS のデバッグ情報をイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect im

IM トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect im** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect im *map_name*

no inspect im *map_name*

構文の説明

map_name	IM マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect im コマンドは、IM プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4
```

```
hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
match protocol	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

inspect ipsec-pass-thru

IPSec Pass Thru インスペクションをイネーブルにするには、クラス マップ コンフィギュレーション モードで **inspect ipsec-pass-thru** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

構文の説明

map_name	（任意）IPSec Pass Thru マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

inspect ipsec-pass-thru コマンドは、アプリケーション インスペクションをイネーブルまたはディセーブルにします。IPSec Pass Through アプリケーション インスペクションによって、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）トラフィックか AH（IP プロトコル 51）トラフィックまたはその両方の便利なトラバーサルが提供されます。このインスペクションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

インスペクションのパラメータの定義に使用する特定のマップを識別するには、IPSec Pass Through パラメータ マップを使用します。パラメータ コンフィギュレーションにアクセスするには、**policy-map type inspect** コマンドを使用します。このコンフィギュレーションで、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーションでは、クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

class-map、**policy-map**、および **service-policy** の各コマンドを使用してトラフィックのクラスを定義し、**inspect** コマンドをクラスに適用して、ポリシーを 1 つまたは複数のインターフェイスに適用します。定義したパラメータ マップは、**inspect IPSec-pass-thru** コマンドで使用されたときにイネーブルになります。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

（注）　ASA 7.0 では、**inspect ipsec-pass-thru** コマンドは ESP トラフィックの通過のみ許可していました。最新バージョンで同じ動作を保持するために、**inspect ipsec-pass-thru** コマンドが引数なしで指定されている場合は、ESP を許可するデフォルト マップが作成され、付加されます。このマップは **show running-config all** コマンドの出力で確認できます。

例

次に、アクセス リストを使用して IKE トラフィックを識別し、IPSec Pass Thru パラメータ マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
match protocol	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

inspect mgcp

MGCP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect mgcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

構文の説明

map_name	（任意）MGCP マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

MGCP を使用するには、通常、2 つ以上の **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つはコール エージェントがコマンドを受信するポート用です。一般的に、コール エージェントはゲートウェイのデフォルト MGCP ポート 2427 にコマンドを送信し、ゲートウェイはコール エージェントのデフォルト MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部コール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。

メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。

- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 *soft PBX* インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。

（注） MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、セキュリティ アプライアンス を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

1 つ以上のコール エージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** および **gateway** コマンドを使用します。コマンド キューで一度に許可される MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect mgcp** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect mgcp** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、MGCP トラフィックを指定し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
```

```
hostname(config)# service-policy inbound_policy interface outside
```

このコンフィギュレーションでは、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 で、10.10.10.116 と 10.10.10.117 の両方のゲートウェイを制御できるようにします。キューに入れることができる MGCP コマンドの最大数は 150 です。

すべてのインターフェイスに対して MGCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug mgcp	MGCP のデバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	セキュリティ アプライアンスを通じて確立された MGCP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect mmp

MMP インスペクション エンジンを設定するには、クラス コンフィギュレーション モードで **inspect mmp** コマンドを使用します。

MMP インスペクションを削除するには、このコマンドの **no** 形式を使用します。

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

構文の説明

name	TLS プロキシ インスタンス名を指定します。
tls-proxy	MMP インスペクションに対して TLS プロキシをイネーブルにします。MMP プロトコルではさらに TCP トランスポートも使用できますが、CUMA クライアントでは TLS トランスポートしかサポートしていません。そのため、MMP インスペクションをイネーブルにするには tls-proxy キーワードが必要です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

ASA には、CUMA Mobile Multiplexing Protocol（MMP）を検証するインスペクション エンジンが含まれています。MMP は、CUMA クライアントとサーバ間でデータ エンティティを送信するためのデータ トランスポート プロトコルです。ASA が CUMA クライアントとサーバの間に配置されており、MMP パケットのインスペクションが必要な場合は、**inspect mmp** コマンドを使用します。

MMP トラフィックは TLS 接続でしか転送できないため、MMP インスペクションは TLS プロキシとともにイネーブルにする必要があります。

例

次に、**inspect mmp** コマンドを使用して MMP トラフィックを検査する例を示します。

```
hostname(config)# class-map mmp
hostname(config-cmap)# match port tcp eq 5443
hostname(config-cmap)# exit
hostname(config)# policy-map mmp-policy
hostname(config-pmap)# class mmp
hostname(config-pmap-c)# inspect mmp tls-proxy myproxy
```

```
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy mmp-policy interface outside
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを設定します。
debug mmp	MMP 検査イベントを表示します。

inspect netbios

NetBIOS アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect netbios** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

構文の説明

map_name	（任意）NetBIOS マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次に、NetBIOS インスペクション ポリシー マップを定義する例を示します。

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect pptp

PPTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect pptp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect pptp

no inspect pptp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行*されません*。

具体的には、セキュリティ アプライアンスは、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始されたヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザ PC です。

例

次の例に示すように、PPTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

すべてのインターフェイスに対して PPTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug pptp	PPTP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect radius-accouting

RADIUS アカウンティング インスペクションをイネーブルまたはディセーブルにしたり、トラフィックまたはトンネルを制御するためのマップを定義したりするには、クラス コンフィギュレーション モードで **inspect radius-accounting** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

構文の説明

map_name	（任意）RADIUS アカウンティング マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティングのパラメータの定義に使用する特定のマップを作成するには、**radius-accounting** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードを開始して、特定のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**send**、**host**、**validate-attribute**、**enable gprs**、および **timeout users** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのコマンドには、**parameter** モードからアクセスできます。

RADIUS アカウンティング マップを定義した後、**inspect gtp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

（注）　**inspect radius-accounting** コマンドは、**class-map type management** コマンドとのみ使用できます。

例

次に、アクセス リストを使用して RADIUS アカウンティング トラフィックを識別し、RADIUS アカウンティング マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# policy-map type inspect radius-accountin ra
```

（注） この例では、デフォルト値で RADIUS アカウンティング インスペクションをイネーブルにします。デフォルト値を変更するには、**parameters** コマンドのページと、RADIUS アカウンティング コンフィギュレーション モードで入力する各コマンドのコマンド ページを参照してください。

関連コマンド

コマンド	説明
parameters	セキュリティ アクションを適用するトラフィック クラスを定義します。
class-map type management	アクションを適用するセキュリティ アプライアンス宛てのレイヤ 3 またはレイヤ 4 管理トラフィックを識別します。
show service-policy および **clear service-policy**	サービス ポリシー設定の表示とクリアを行います。
debug inspect radius-accounting	RADIUS アカウンティング インスペクションをデバッグします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect rsh

RSH アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect rsh** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect rsh

no inspect rsh

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次の例に示すように、RSH インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（514）上の RSH トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

すべてのインターフェイスに対して RSH インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect rtsp

RTSP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect rtsp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

構文の説明

map_name	（任意）RTSP マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect rtsp コマンドを使用すると、セキュリティ アプライアンスで RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注） Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートします。この TCP コントロール チャネルは、クライアントに設定されているトランスポート モードに応じて、オーディオ / ビデオ トラフィックの送信に使用されるデータ チャネルをネゴシエートするために使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

セキュリティ アプライアンスは、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合は、サーバは セキュリティ アプライアンスとの相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、セキュリティ アプライアンス は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアントとサーバのポートを SETUP 応答メッセージ内に含める必要があるとは規定していないため、セキュリティ アプライアンスで状態を保持し、SETUP メッセージに含まれているクライアント ポートを記憶しておく必要があります。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RealPlayer の使用方法

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、サーバからクライアントまたはその逆の **access-list** コマンド ステートメントを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP] [Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。セキュリティ アプライアンスで、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、セキュリティ アプライアンスで、**inspect rtsp** *port* コマンド ステートメントを追加します。

制限事項

inspect rtsp コマンドに適用される制約事項は次のとおりです。

- セキュリティ アプライアンス は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- セキュリティ アプライアンス には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- Cisco IP/TV の場合、セキュリティ アプライアンスがメッセージの SDP 部分に対して実行する NAT の数は、Content Manager のプログラム リストの数に比例します（プログラム リストごとに少なくとも 6 個の埋め込み IP アドレスを設定できます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。
- HTTP を介して配信されるメディア ストリームは、RTSP アプリケーション インスペクションではサポートされません。これは、RTSP インスペクションが HTTP クローキング（HTTP でラップされた RTSP）をサポートしていないためです。

例

次の例に示すように、RTSP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（554 および 8554）上の RTSP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-traffic
```

```
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

すべてのインターフェイスに対して RTSP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug rtsp	RTSP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect sip

SIP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect sip** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	指定したインスペクション セッションの Phone Proxy をイネーブルにします。
sip_map	SIP ポリシー マップ名を指定します。
tls-proxy *proxy_name*	指定されたインスペクション セッションで TLS プロキシをイネーブルにします。キーワード tls-proxy をレイヤ 7 ポリシー マップ名として使用することはできません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

SIP のデフォルトのポート割り当ては 5060 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	**tls-proxy** キーワードが追加されました。
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SIP は、IETF で定義されているように、VoIP コールをイネーブルにします。SIP は SDP と連携して、コール シグナリングを行います。SDP はメディア ストリームの詳細を指定します。SIP を使用すると、セキュリティ アプライアンスですべての SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディ

アの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP インスペクションは、それらの埋め込まれた IP アドレスに NAT を適用します。

（注）　リモート エンドポイントが、セキュリティ アプライアンスで保護されているネットワーク上の SIP プロキシに対して登録を試行すると、登録は非常に特殊な条件で失敗します。この条件とは、リモート エンドポイントに PAT が設定されていること、SIP レジストラ サーバが外部ネットワーク上にあること、およびエンドポイントによってプロキシ サーバに送信された REGISTER メッセージの contact フィールドにポートがないことです。

インスタント メッセージング

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定した SIP タイムアウト値に応じてタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注）　現在は、チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

技術的詳細

SIP インスペクションは、SIP テキストベースのメッセージに対して NAT を実行し、メッセージの SDP 部分のコンテンツ長を再計算して、パケット長およびチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションには、コールと送信元および宛先を識別する SIP ペイロードの CALL_ID、FROM、TO インデックスが含まれるデータベースがあります。このデータベースに格納されるのは、SDP メディア情報フィールドに格納されていたメディア アドレスおよびメディア ポートと、メディア タイプです。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。RTP/RTCP 接続は、これらのメディア アドレスおよびポートを使用して、2 つのエンドポイント間で開かれます。

最初のコール設定（INVITE）メッセージでは、既知のポート 5060 を使用する必要があります。ただし、後続のメッセージではこのポート番号を使用しないこともあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。この処理は、メッセージを SIP アプリケーションに到達させて、NAT を実行するために行われます。

コールが設定されると、SIP セッションは「一時的な」状態にあると見なされます。この状態は、宛先エンドポイントがリッスンしている RTP メディア アドレスとポートを示す Response メッセージが受信されるまで維持されます。1 分以内に応答メッセージを受信できなかった場合は、シグナリング接続が切断されます。

最後のハンドシェイクが行われると、コール状態はアクティブに移り、シグナリング接続は、BYE メッセージが受信されるまで維持されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスへの非請求 RTP/RTCP UDP パケットは、セキュリティ アプライアンスのコンフィギュレーションで特別に許可されていない限りセキュリティ アプライアンスを通過しません。

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect sip** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect sip** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SIP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（5060）上の SIP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

すべてのインターフェイスに対して SIP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
debug sip	SIP のデバッグ情報をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

inspect skinny

SCCP（Skinny）アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect skinny** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	指定したインスペクション セッションの Phone Proxy をイネーブルにします。
skinny_map	skinny ポリシー マップ名を指定します。
tls-proxy *proxy_name*	指定されたインスペクション セッションで TLS プロキシをイネーブルにします。キーワード tls-proxy をレイヤ 7 ポリシー マップ名として使用することはできません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	キーワード **tls-proxy** が追加されました。
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Skinny（または Simple）Client Control Protocol（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。SCCP クライアントは、Cisco CallManager とともに使用することで、H.323 準拠の端末と相互運用できます。セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。アプリケーション層ソフトウェアの機能で、SCCP シグナリング パケットの NAT を提供することにより、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できるようになります。

SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。セキュリティ アプライアンスでは、バージョン 3.3.2 までのすべてのバージョンをサポートしています。は、SCCP に対して PAT と NAT の両方のサポートを提供しています。IP 電話で使用するグローバル IP アドレスの数を制限している場合は、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックでは SCCP が使用され、特別なコンフィギュレーションがない限り SCCP インスペクションで処理されます。セキュリティ アプライアンスでは、セキュリティ アプライアンスで TFTP サーバの場所を Cisco IP Phone および他の DHCP クライアントに送信できるようにする、DHCP オプション 150 および 66 もサポートしています。詳細については、**dhcp-server** コマンドを参照してください。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。ID スタティック エントリを使用すると、よりセキュリティの高いインターフェイスに配置されている Cisco CallManager で Cisco IP Phone からの登録を受け付けられるようになります。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、これは「ID」スタティック エントリである必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べてセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、アクセス リストやスタティック エントリは必要ありません。

制限事項

SCCP に対する現在のバージョンの PAT および NAT サポートに適用される制限は、次のとおりです。

- PAT は、**alias** コマンドを使用しているコンフィギュレーションでは動作しません。
- 外部 NAT および PAT はサポート **されません**。

（注） SCCP コールのステートフル フェールオーバーは、コール設定の最中のコールを除いて、サポートされるようになりました。

内部 Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスまたはポートに設定されている場合、セキュリティ アプライアンスでは、現在、TFTP 経由で転送されるファイル コンテンツに対する NAT または PAT をサポートしていないため、外部 Cisco IP Phone の登録は失敗します。セキュリティ アプライアンスでは TFTP メッセージの NAT をサポートしており、TFTP ファイルがセキュリティ アプライアンスを通過するためのピンホールを開きますが、電話機の登録時に TFTP を使用して転送される Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager IP アドレスおよびポートは、セキュリティ アプライアンスでは変換できません。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect skinny** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect skinny** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SCCP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（2000）上の SCCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

すべてのインターフェイスに対して SCCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
show skinny	セキュリティ アプライアンスを通じて確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

inspect snmp

SNMP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect snmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect snmp *map_name*

no inspect snmp *map_name*

構文の説明

map_name	SNMP マップ名です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SNMP マップで指定した設定を使用して SNMP インスペクションをイネーブルにするには、inspect snmp コマンドを使用します。SNMP マップは **snmp-map** コマンドを使用して作成します。SNMP トラフィックを特定のバージョンの SNMP に制限するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。

以前のバージョンの SNMP はセキュリティが低いため、SNMP トラフィックをバージョン 2 に制限するようにセキュリティ ポリシーで要求する場合があります。SNMP の特定のバージョンを拒否するには、**snmp-map** コマンドを使用して作成する SNMP マップで、**deny version** コマンドを使用します。SNMP マップを設定した後、**inspect snmp** コマンドを使用してマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスにこのマップを適用します。

例

次に、SNMP トラフィックを識別し、SNMP マップを定義して、ポリシーを定義し、SNMP インスペクションをイネーブルにして、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
```

```
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

すべてのインターフェイスに対してストリクト snmp アプリケーション インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect sqlnet

Oracle SQL*Net アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect sqlnet** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sqlnet

no inspect sqlnet

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

デフォルトのポート割り当ては 1521 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。セキュリティ アプライアンスはこれらのパケットを処理して、セキュリティ アプライアンス のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。SQL*Net インスペクションを一連のポート番号に適用するには、**class-map** コマンドを使用します。

（注） SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

セキュリティ アプライアンスは、すべてのアドレスの NAT を実行し、パケット内のすべての埋め込みポートを検索して、SQL*Net バージョン 1 用に開きます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長がゼロの Redirect メッセージがセキュリティ アプライアンスを通過すると、後続の Data または Redirect メッセージの NAT が実行され、ポートがダイナミックに開かれることを想定するフラグが接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスの NAT が実行され、ポート接続が開かれます。

例

次の例に示すように、SQL*Net インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1521）上の SQL*Net トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

すべてのインターフェイスに対して SQL*Net インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug sqlnet	SQL*Net のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SQL*net など、さまざまな接続タイプの接続状態を表示します。

inspect sunrpc

Sun RPC アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc

no inspect sunrpc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Sun RPC アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、ポリシー マップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。このモードにアクセスするには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc コマンドは、Sun RPC プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはシステムの任意のポートで実行できます。クライアントがサーバ上の Sun RPC サービスにアクセスしようとする場合には、サービスが実行されているポートを検出する必要があります。これを行うには、既知のポート 111 でポートマッパー プロセスを照会します。

クライアントはサービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点より、クライアント プログラムは Sun RPC クエリーをその新しいポートに送信します。サーバから応答が送信されると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

（注）　Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

例

次の例に示すように、RPC インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（111）上の RPC トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して RPC インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されているコンフィギュレーションを削除します。
clear sunrpc-server active	Sun RPC アプリケーション インスペクションによって、NFS または NIS などの特定のサービス用に開けられているピンホールをクリアします。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションの情報を表示します。
sunrpc-server	NFS または NIS などの Sun RPC サービス用に、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービス用に開けられているピンホールを表示します。

inspect tftp

TFTP アプリケーション インスペクションをディセーブルにしたり、ディセーブルになっている場合にイネーブルにしたりするには、クラス コンフィギュレーション モードで **inspect tftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect tftp

no inspect tftp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

デフォルトのポート割り当ては 69 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RFC 1350 に規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバとクライアント間でファイルを読み書きするための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP Read Request（RRQ; 読み取り要求）、Write Request（WRQ; 書き込み要求）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

例

次の例に示すように、TFTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（69）上の TFTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

すべてのインターフェイスに対して TFTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect waas

WAAS アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect waas** コマンドを使用します。クラス コンフィギュレーション モードは、ポリシー マップ コンフィギュレーション モードからアクセス可能です。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect waas

no inspect waas

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、WAAS アプリケーション インスペクションをイネーブルにする方法を示します。

```
hostname(config-pmap-c)# inspect waas
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect xdmcp

XDMCP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect xdmcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect xdmcp

no inspect xdmcp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、セキュリティ アプライアンスで **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

例

次の例に示すように、XDMCP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（177）上の XDMCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

すべてのインターフェイスに対して XDMCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug xdmcp	XDMCP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

CHAPTER 16

intercept-dhcp コマンド～ issuer-name コマンド

intercept-dhcp

DHCP 代行受信をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **intercept-dhcp enable** コマンドを使用します。DHCP 代行受信をディセーブルにするには、**intercept-dhcp disable** コマンドを使用します。実行コンフィギュレーションから intercept-dhcp 属性を削除し、ユーザがデフォルトまたはその他のグループ ポリシーから DHCP 代行受信コンフィギュレーションを継承できるようにするには、**no intercept-dhcp** コマンドを使用します。

intercept-dhcp *netmask* {**enable** | **disable**}

no intercept-dhcp

構文の説明

disable	DHCP 代行受信をディセーブルにします。
enable	DHCP 代行受信をイネーブルにします。
netmask	トンネル IP アドレスのサブネット マスクを提供します。

デフォルト

DHCP 代行受信はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、セキュリティ アプライアンスで送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信によって Microsoft XP クライアントは、セキュリティ アプライアンスでスプリット トンネリングを使用できるようになります。セキュリティ アプライアンスは、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

例

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

interface

インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。インターフェイス コンフィギュレーション モードでは、インターフェイスのタイプおよびセキュリティ コンテキスト モードに応じて、ハードウェアの設定（物理インターフェイスの場合）、名前の割り当て、VLAN の割り当て、IP アドレスの割り当てをはじめ、数多くの設定を行うことができます。

マルチ コンテキスト モードでは、**allocate-interface** コマンドを使用してマッピング名が割り当てられた場合、そのマッピング名の指定が必要になることがあります。

すべてのモデルで、物理インターフェイスのパラメータを設定できます。

ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルを除くすべてのモデルで、論理冗長インターフェイスを作成できます。

ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルを除くすべてのモデルで、VLAN に割り当てられる論理サブインターフェイスを作成できます。組み込みスイッチを搭載したモデルには、VLAN インターフェイスに割り当てることができるスイッチ ポート（このコマンドで物理インターフェイスと呼んでいるもの）を備えているものがあります。この場合、VLAN のサブインターフェイスを作成するのではなく、物理インターフェイスから独立した VLAN インターフェイスを作成します。その後、VLAN インターフェイスに 1 つ以上の物理インターフェイスを割り当てることができます。

冗長インターフェイス、サブインターフェイス、または VLAN インターフェイスを削除するには、このコマンドの **no** 形式を使用します。物理インターフェイスまたはマッピングされているインターフェイスは削除できません。

物理インターフェイスの場合（全モデルが対象）：

interface *physical_interface*

冗長インターフェイスの場合（組み込みスイッチを搭載したモデルには使用不可）：

interface redundant *number*

no interface redundant *number*

サブインターフェイスの場合（組み込みスイッチを搭載したモデルには使用不可）：

interface {*physical_interface* | **redundant** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number*}**.***subinterface*

VLAN インターフェイスの場合（組み込みスイッチを搭載したモデルが対象）：

interface vlan *number*

no interface vlan *number*

マルチ コンテキスト モードの場合（マッピング名が割り当てられているとき）：

interface *mapped_name*

構文の説明

mapped_name	マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名が割り当てられている場合は、マッピング名を指定します。
physical_interface	*type*[*slot*/]*port* という形式で物理インターフェイスのタイプ、スロット、およびポート番号を指定します。タイプとスロット/ポート間のスペースは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • **gigabitethernet** • **management**（ASA 5500 のみ） PIX 500 シリーズ セキュリティ アプライアンスでは、タイプの後ろにポート番号を入力します（**ethernet0** など）。 ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、スロット/ポート（たとえば、**gigabitethernet 0/1**. の前に来るタイプを入力します。シャーシに組み込まれているインターフェイスは、スロット 0 に割り当てられ、4GE SSM（または組み込み 4GE SSM）のインターフェイスはスロット 1 に割り当てられます。 管理インターフェイスは、管理トラフィック専用のファスト イーサネット インターフェイスであり、**management 0/0** のように指定します。ただし、必要に応じて通過トラフィック用に使用することもできます（**management-only** コマンドを参照）。トランスペアレント ファイア ウォール モードでは、通過トラフィックに許可されている 2 つのインターフェイスに加えて、管理インターフェイスを使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードの各セキュリティ コンテキストでの管理を実現できます。 インターフェイスのタイプ、スロット、およびポート番号を確認するには、モデルに付属のハードウェア マニュアルを参照してください。
redundant *number*	論理冗長インターフェイスを指定します。*number* には 1 ～ 8 の値を指定します。冗長インターフェイスは、アクティブ物理インターフェイスとスタンバイ物理インターフェイスのペアとなっています（**member-interface** コマンドを参照）。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。 すべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。 **redundant** と ID 間のスペースは任意です。
subinterface	論理サブインターフェイスに指定されている 1 ～ 4294967293 の整数を指定します。サブインターフェイスの最大数は、セキュリティ アプライアンス モデルによって異なります。サブインターフェイスは、ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルには使用できません。プラットフォームあたりのサブインターフェイス（または VLAN）の最大数については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。
vlan *number*	組み込みスイッチを搭載したモデルの場合、VLAN ID を 1 ～ 4090 の範囲で指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスはすべての物理インターフェイスを対象に **interface** コマンドを自動的に生成します。

マルチ コンテキスト モードでは、セキュリティ アプライアンスは **allocate-interface** コマンドを使用して、コンテキストに割り当てられているすべてのインターフェイスを対象に **interface** コマンドを自動的に生成します。

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、サブインターフェイスの新しい命名規則に対応し、インターフェイス コンフィギュレーション モードでは引数が独立したコマンドとなるように変更されました。
7.2(1)	**interface vlan** コマンドが、ASA 5505 適応型セキュリティ アプライアンスでの組み込みスイッチをサポートするために追加されました。
8.0(2)	**interface redundant** コマンドが追加されました。

使用上のガイドライン

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。サブインターフェイスの場合は、**vlan** コマンドも設定します。スイッチ物理インターフェイスの場合、**switchport access vlan** コマンドを使用して、物理インターフェイスを VLAN インターフェイスに割り当てます。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに「inside」という名前を付け、**security-level** コマンドを使用してセキュリティ レベルを明示的に設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

マルチ コンテキスト モードのガイドライン

- 各コンテキスト内からコンテキスト インターフェイスを設定します。
- システム コンフィギュレーションでコンテキストにすでに割り当てたコンテキスト インターフェイスを設定します。それ以外のインターフェイスは使用できません。
- システム コンフィギュレーションでイーサネット設定、冗長インターフェイス、およびサブインターフェイスを設定します。それ以外のコンフィギュレーションは使用できません。フェールオーバー インターフェイスは例外で、システム コンフィギュレーションに設定されます。このコマンドでフェールオーバー インターフェイスを設定しないでください。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。

サブインターフェイスのガイドライン

- 最大サブインターフェイス：プラットフォームに許可するサブインターフェイスの数を決定するには、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』でライセンス情報を参照してください。
- 物理インターフェイスでのタグなしパケットの阻止：サブインターフェイスを使用する場合は、物理インターフェイスでは一般にトラフィックを通過させないようにします。物理インターフェイスではタグなしパケットが通過してしまうためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスまたは冗長インターフェイスをイネーブルにする必要があるため、**nameif** コマンドを除外して物理インターフェイスまたは冗長インターフェイスでトラフィックを通過させないようにします。物理インターフェイスまたは冗長インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

冗長インターフェイスのガイドライン

- フェールオーバーのガイドライン：
  - フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的なコンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
  - フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
  - **monitor-interface** コマンドを使用して、フェールオーバーの冗長インターフェイスをモニタできます。その際、論理冗長インターフェイス名を参照してください。
  - アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

- 冗長インターフェイスの MAC アドレス：冗長インターフェイスは、最初に追加した物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、メンバー インターフェイスの MAC アドレスとは関係なく使用される MAC アドレスを冗長インターフェイスに割り当てることができます（**mac-address** コマンドまたは **mac-address auto** コマンドを参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合は、同じ MAC アドレスが維持されるため、トラフィックが妨げられることはありません。
- 物理インターフェイスのガイドライン：メンバー インターフェイスを追加するときには、次のガイドラインに従ってください。
  - 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
  - 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。この場合、まず **no nameif** コマンドを使用して名前を削除する必要があります。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

  - 冗長インターフェイス ペアの一部である物理インターフェイスに使用できるコンフィギュレーションのみが物理パラメータ（**speed** コマンド、**duplex** コマンド、**description** コマンド、**shutdown** コマンドなど）です。また、**default** や **help** などの実行時コマンドを入力することもできます。
  - アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

組み込みスイッチのガイドライン

組み込みスイッチを搭載したモデルの場合、物理インターフェイス専用の物理パラメータおよびスイッチ パラメータ（VLAN 割り当てを含む）を設定します。VLAN インターフェイスにはその他のすべてのパラメータを設定します。

トランスペアレント ファイアウォール モードの ASA 5505 適応型セキュリティ アプライアンスの場合､基本ライセンスで 2 つのアクティブ VLAN と Security Plus ライセンスで 3 つのアクティブ VLAN を設定でき、そのうちの 1 つをフェールオーバー用にする必要があります。ルーテッド モードでは、基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。VLAN は、アクティブ VLAN の数を制限してライセンスに準拠している限り、必要な数だけ設定できます。基本ライセンスの場合、3 つめの VLAN は他の 1 つの VLAN にのみトラフィックを開始するように設定できます。3 つめの VLAN を制限するには、**no forward interface** コマンドを使用します。Security Plus ライセンスでは、通常のトラフィック用に 3 つの VLAN インターフェイス、フェールオーバー用に 1 つの VLAN インターフェイス、および ISP へのバックアップ リンクとして 1 つの VLAN インターフェイスを設定できます。ただし、フェールオーバー VLAN インターフェイスは、**interface vlan** コマンドでは設定されません。フェールオーバー VLAN ID に物理インターフェイスを割り当てた後、**failover lan** コマンドを使用して VLAN インターフェイスを作成し、設定します。ISP へのバックアップ リンクを識別するには、プライマリ VLAN コンフィギュレーションで **backup interface** コマンドを使用します。このインターフェイスは、プライマリ インターフェイスで障害が発生しない限り、トラフィックを通過させません。詳細については、**backup interface** コマンドを参照してください。

管理専用インターフェイス

ASA 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 という専用の管理インターフェイスが含まれ、セキュリティ アプライアンスへのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の場合、管理専用モードをディセーブルにできるため、このインターフェイスは他のインターフェイスと同じくトラフィックを通過させることができます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。

例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次に、コンテキスト コンフィギュレーション用にマルチ コンテキスト モードでパラメータを設定する例を示します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

次の例では、3 つの VLAN インターフェイスを設定します。3 つめのホーム インターフェイスは、トラフィックをワーク インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
```

```
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

次に、**failover lan** コマンドを使用して別途設定されるフェールオーバー インターフェイスを含め、5 つの VLAN インターフェイスを設定する例を示します。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
```

```
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

次の例では、2 つの冗長インターフェイスを作成します。

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
member-interface	インターフェイスを冗長インターフェイスに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN を割り当てます。

interface（vpn ロードバランシング）

VPN ロード バランシングの仮想クラスタで VPN ロード バランシング用にデフォルト以外のパブリック インターフェイスまたはプライベート インターフェイスを指定するには、VPN ロード バランシング モードで **interface** コマンドを使用します。このインターフェイス指定を削除し、デフォルトのインターフェイスに戻すには、このコマンドの **no** 形式を使用します。

interface {**lbprivate** | **lbpublic**} *interface-name*]

no interface {**lbprivate** | **lbpublic**}

構文の説明

interface-name	VPN ロード バランシング クラスタのパブリック インターフェイスまたはプライベート インターフェイスとして設定されるインターフェイスの名前。
lbprivate	このコマンドが VPN ロード バランシングのプライベート インターフェイスを設定することを指定します。
lbpublic	このコマンドが VPN ロード バランシングのパブリック インターフェイスを設定することを指定します。

デフォルト

interface コマンドを省略した場合、**lbprivate** インターフェイスはデフォルトで **inside** に設定され、**lbpublic** インターフェイスはデフォルトで **outside** に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
vpn ロード バランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始しておく必要があります。

また、あらかじめ **interface**、**ip address**、**nameif** の各コマンドを使用して、このコマンドで指定するインターフェイスを設定し、名前を割り当てておく必要があります。

このコマンドの no 形式は、インターフェイスをデフォルトの状態に戻します。

例

次に、**vpn load-balancing** コマンド シーケンスの一例を示します。この中の **interface** コマンドでは、クラスタのプライベート インターフェイスをデフォルト（inside）に戻す「test」インターフェイスとして、クラスタのパブリック インターフェイスを指定しています。

```
hostname(config)# interface GigabitEthernet 0/1
```

```
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

interface-policy

モニタリングでインターフェイスの障害を検出する際にフェールオーバーのポリシーを指定するには、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

構文の説明

num	パーセンテージとして使用するときには 1 ～ 100 の数値を指定し、そうでなければインターフェイスの最大数として 1 を指定します。
%	（任意）*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

ユニットに **failover interface-policy** コマンドが設定されている場合は、**interface-policy** フェールオーバー グループ コマンドのデフォルトが設定値であると見なされます。そうでない場合、*num* は 1 となります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が設定したポリシーを満たし、他のセキュリティ アプライアンスが正しく機能している場合、セキュリティ アプライアンスが自らを障害発生としてマークし、フェールオーバーが発生することがあります（アクティブなセキュリティ アプライアンスで障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
```

```
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover interface-policy	インターフェイス モニタリング ポリシーを設定します。
monitor-interface	フェールオーバーのためにモニタ対象にするインターフェイスを指定します。

internal-password

クライアントレス SSL VPN ポータル ページで追加パスワード フィールドを表示するには、webvpn コンフィギュレーション モードで **internal-password** コマンドを使用します。この追加パスワードは、セキュリティ アプライアンスが SSO を許可しているファイル サーバに対してユーザを認証するのに使用されます。

内部パスワードの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

internal-password enable

no internal password

構文の説明

enable	内部パスワードの使用をイネーブルにします。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

イネーブルにした場合、エンド ユーザはクライアントレス SSL VPN セッションにログインするときに 2 つめのパスワードを入力します。クライアントレス SSL VPN サーバは、HTTPS を使用して、ユーザ名やパスワードなどの SSO 認証要求を認証サーバに送信します。認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザに代わってセキュリティ アプライアンスに保持され、ユーザを認証して SSO サーバによって保護されたドメイン内の Web サイトを保護するのに使用されます。

内部パスワード機能は、内部パスワードを SSL VPN パスワードとは異なるものにする場合に便利です。特に、セキュリティ アプライアンスへの認証にワンタイム パスワードを使用し、内部サイトの認証に別のパスワードを使用できます。

例

次に、内部パスワードをイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# internal password enable
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSLVPN 接続の属性を設定できます。

interval maximum

DDNS 更新方式による更新試行の最大間隔を設定するには、DDNS 更新方式モードで **interval** コマンドを使用します。実行コンフィギュレーションから DDNS 更新方式の間隔を削除するには、このコマンドの **no** 形式を使用します。

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

構文の説明

days	更新試行間の日数を 0 ～ 364 の範囲で指定します。
hours	更新試行間の時間数を 0 ～ 23 の範囲で指定します。
minutes	更新試行間の分数を 0 ～ 59 の範囲で指定します。
seconds	更新試行間の秒数を 0 ～ 59 の範囲で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DDNS 更新方式 コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

日、時間、分、および秒を足すと、間隔の合計時間になります。

例

次に、3 分 15 秒ごとに更新を試行する方式を ddns-2 という名前で設定する例を示します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# interval maximum 0 0 3 15
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。

コマンド	説明
ddns update method (グローバル コンフィギュレーション モード)	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。

invalid-ack

ACK が無効になっているパケットに対するアクションを設定するには、tcp-map コンフィギュレーション モードで **invalid-ack** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

invalid-ack {**allow** | **drop**}

no invalid-ack

構文の説明

allow	ACK が無効になっているパケットを許可します。
drop	ACK が無効になっているパケットをドロップします。

デフォルト

デフォルト アクションは、ACK が無効になっているパケットをドロップすることです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **invalid-ack**：tcp-map コンフィギュレーション モードでは、**invalid-ack** コマンドをはじめ多数のコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

次のような場合に無効な ACK が検出される可能性があります。

- TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。

- 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。

（注）　無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

例

次に、ACK が無効になっているパケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# invalid-ack allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

ip address

インターフェイス（ルーテッド モード）または管理アドレス（トランスペアレント モード）の IP アドレスを設定するには、**ip address** コマンドを使用します。ルーテッド モードの場合は、インターフェイス コンフィギュレーション モードでこのコマンドを入力します。トランスペアレント モードの場合は、グローバル コンフィギュレーション モードでこのコマンドを入力します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。このコマンドはこの他、フェールオーバーのスタンバイ アドレスを設定します。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

no ip address [*ip_address*]

構文の説明

ip_address	インターフェイスの IP アドレス（ルーテッド モード）または管理 IP アドレス（トランスペアレント モード）。
mask	（任意）IP アドレスのサブネット マスク。マスクを設定しない場合、セキュリティ アプライアンスでは IP アドレス クラスのデフォルト マスクが使用されます。
standby *ip_address*	（任意）フェールオーバーのスタンバイ ユニットの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	ルーテッド モードの場合、このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスはそれぞれ固有のサブネットに存在する必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイスにある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。セキュリティ アプライアンスに必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要になるのは、セキュリティ アプライアンスがシステム メッセージや AAA サーバとの通信などセキュリティ アプライアンスで発信されるトラフィックの送信元アドレスとしてこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネットに存在する必要があります。

例

次に、2 つのインターフェイスの IP アドレスおよびスタンバイ アドレスを設定する例を示します。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

次に、トランスペアレント ファイアウォールの管理アドレスおよびスタンバイ アドレスを設定する例を示します。

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address dhcp	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip address dhcp

DHCP を使用してインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。このインターフェイスの DHCP クライアントをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address dhcp [**setroute**]

no ip address dhcp

構文の説明

setroute	（任意）セキュリティ アプライアンスが DHCP サーバから提供されたデフォルト ルートを使用できるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。このコマンドは、外部インターフェイスだけでなく、任意のインターフェイスもイネーブルにできます。

使用上のガイドライン

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

（注）　セキュリティ アプライアンスは、タイムアウトが 32 秒未満のリースを拒否します。

例

次に、gigabitethernet0/1 インターフェイスで DHCP をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイア ウォールの管理 IP アドレスを設定します。
show ip address dhcp	DHCP サーバから取得された IP アドレスを示します。

ip address pppoe

PPPoE をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip address pppoe** コマンドを使用します。PPPoE をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

構文の説明

ip_address	IP アドレスを PPPoE サーバから受信するのではなく手動で設定します。
mask	IP アドレスのサブネット マスクを指定します。マスクを設定しない場合、セキュリティ アプライアンスでは IP アドレス クラスのデフォルト マスクが使用されます。
setroute	セキュリティ アプライアンスが、PPPoE サーバから提供されるデフォルト ルートを使用できるようにします。PPPoE サーバがデフォルト ルートを送信しない場合、セキュリティ アプライアンスはアクセス コンセントレータのアドレスをゲートウェイとするデフォルト ルートを作成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに割り当てる認証方式を提供します。ISP は、既存のリモート アクセス インフラストラクチャを使用して高速ブロードバンド アクセスをサポートするためと、顧客の使い勝手向上のために、PPPoE を配置します。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドでユーザ名、パスワード、および認証プロトコルを設定します。複数のインターフェイスでこのコマンドをイネーブルにした場合（たとえば、ISP へのバックアップ リンク用）は、**pppoe client vpdn group** コマンドを使用して、必要に応じて各インターフェイスをそれぞれ異なる VPDN グループに割り当てることができます。

最大伝送単位（MTU）サイズは、自動的に 1492 バイトに設定されます。これは、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

PPPoE セッションをリセットして再起動するには、このコマンドを再入力します。

このコマンドは、**ip address** コマンドまたは **ip address dhcp** コマンドと同時には設定できません。

例

次に、GigabitEthernet 0/1 インターフェイスで PPPoE をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address pppoe
hostname(config-if)# no shutdown
```

次に、PPPoE インターフェイスの IP アドレスを手動で設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレスを設定します。
pppoe client vpdn group	このインターフェイスを特定の VPDN グループに割り当てます。
show ip address pppoe	PPPoE サーバから取得された IP アドレスを表示します。
vpdn group	～を作成します。

ip-address-privacy

IP アドレスのプライバシーをイネーブルにするには、パラメータ コンフィギュレーション モードで **ip-address-privacy** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip-address-privacy

no ip-address-privacy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由する IP アドレスのプライバシーをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ip-address-privacy
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

ip audit attack

攻撃シグニチャに一致するパケットに対してデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit attack** コマンドを使用します。デフォルト アクションを復元（して接続をリセット）するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

構文の説明

action	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しない場合、セキュリティ アプライアンスではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、送信し、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、攻撃シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームだけを生成するようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit attack** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit attack action alarm reset
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

ip audit info

情報シグニチャに一致するパケットに対してデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit info** コマンドを使用します。デフォルト アクションを復元（してアラームを生成）するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

構文の説明

action	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しない場合、セキュリティ アプライアンスではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、情報シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームを生成し、ドロップするようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit info** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit info action alarm reset
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドのコンフィギュレーションを表示します。

ip audit interface

監査ポリシーをインターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **ip audit interface** コマンドを使用します。インターフェイスからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

構文の説明

interface_name	インターフェイス名を指定します。
policy_name	**ip audit name** コマンドで追加したポリシーの名前。各インターフェイスに **info** ポリシーおよび **attack** ポリシーを割り当てることができます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、監査ポリシーを内部インターフェイスおよび外部インターフェイスに適用する例を示します。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。

コマンド	説明
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドのコンフィギュレーションを表示します。

ip audit name

パケットが定義済みの攻撃シグニチャまたは情報シグニチャに一致したときに実行するアクションを識別する名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

構文の説明

action	（任意）一連のアクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しないと、セキュリティ アプライアンスは **ip audit attack** コマンドおよび **ip audit info** コマンドによって設定されたデフォルト アクションを使用します。
alarm	（任意）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
attack	攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークでの攻撃の一部となる可能性があります。
drop	（任意）パケットをドロップします。
info	情報シグニチャの監査ポリシーを作成します。パケットは、現時点ではネットワークを攻撃していませんが、ポート スイープなど情報収集アクティビティの一部である可能性があります。
name	ポリシーの名前を設定します。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

ip audit attack コマンドおよび **ip audit info** コマンドを使用してデフォルト アクションを変更しなかった場合、攻撃シグニチャおよび情報シグニチャのデフォルト アクションはアラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ポリシーを適用するには、**ip audit interface** コマンドを使用して、そのポリシーをインターフェイスに割り当てます。各インターフェイスに **info** ポリシーおよび **attack** ポリシーを割り当てることができます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

トラフィックがシグニチャに一致し、そのトラフィックに対してアクションを実行する場合は、**shun** コマンドを使用して、問題のホストからの新規接続を拒否し、既存の接続からのパケットの受信を禁止します。

例

次に、内部インターフェイスには攻撃シグニチャおよび情報シグニチャに関するアラームを生成する監査ポリシーを設定し、外部インターフェイスには攻撃に備えて接続をリセットする監査ポリシーを設定する例を示します。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスおよび宛先アドレスでパケットをブロックします。

ip audit signature

監査ポリシーに対してシグニチャをディセーブルにするには、グローバル コンフィギュレーション モードで **ip audit signature** コマンドを使用します。シグニチャを再びイネーブルにするには、このコマンドの **no** 形式を使用します。正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

構文の説明

signature_number	ディセーブルにするシグニチャ番号を指定します。サポートされているシグニチャのリストについては、表 16-1 を参照してください。
disable	シグニチャをディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　表 16-1 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 16-1　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	Informational	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	Informational	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	Informational	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	Informational	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	Informational	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	Informational	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	Informational	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	Attack	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	Attack	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	Attack	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味します。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	Informational	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、最終フラグメント ビットが設定され、さらに（IP オフセット * 8）+（IP データ長）が 65535 を超えている場合、つまり IP オフセット（このフラグメントの元のパケットでの開始位置を表し、かつ 8 バイト単位であるもの）にパケットの残りを加えた値が、IP パケットの最大サイズを超えている IP データグラムを受信するとトリガーします。
3040	400026	TCP NULL flags	Attack	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	Attack	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	Attack	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	Informational	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	Informational	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	Attack	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	Attack	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	Attack	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	Informational	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	Informational	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	Informational	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	Informational	すべてのレコードに対する DNS 要求があるとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6100	400038	RPC Port Registration	Informational	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。
6101	400039	RPC Port Unregistration	Informational	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	Informational	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	Attack	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	YP サーバ デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	Informational	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6180	400049	rexd (remote execution daemon) Attempt	Informational	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	Attack	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

例

次に、シグニチャ 6100 をディセーブルにする例を示します。

```
hostname(config)# ip audit signature 6100 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit signature	**ip audit signature** コマンドのコンフィギュレーションを表示します。

ip-comp

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮をディセーブルにするには、**ip-comp disable** コマンドを使用します。

実行コンフィギュレーションから **ip-comp** 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーの値を継承できます。

ip-comp {**enable** | **disable**}

no ip-comp

構文の説明

disable	IP 圧縮をディセーブルにします。
enable	IP 圧縮をイネーブルにします。

デフォルト

IP 圧縮はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意　データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果セキュリティ アプライアンス全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

例

次に、「FirstGroup」というグループ ポリシーの IP 圧縮をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip local pool

VPN リモート アクセス トンネルに使用される IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

構文の説明

first-address	IP アドレスの範囲における開始アドレスを指定します。
last-address	IP アドレスの範囲における最終アドレスを指定します。
mask *mask*	（任意）アドレス プールのサブネット マスクを指定します。
poolname	IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

VPN クライアントに割り当てられた IP アドレスが標準以外のネットワークに属しているときには、マスク値を指定する必要があります。デフォルト マスクを使用した場合には、データが誤ってルーティングされることがあります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。この結果、VPN クライアントが異なるインターフェイス経由で 10 ネットワーク内の別のサブネットにアクセスする必要がある場合には、ある種のルーティング問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 を介して使用できるようになっているものの、10.10.10.0 ネットワークが VPN トンネルを経由するためインターフェイス 1 で使用できるようになっている場合、VPN クライアントはプリンタ宛てのデータのルーティング先を正確に把握できなくなります。10.10.10.0 と 10.10.100.0 のサブネットは両方とも、10.0.0.0 クラス A ネットワークに分類されるため、プリンタ データが VPN トンネル経由で送信される可能性があります。

例

次に、firstpool という名前で IP アドレス プールを設定する例を示します。開始アドレスは 10.20.30.40 で、最終アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
show running-config ip local pool	IP プール コンフィギュレーションを表示します。特定の IP アドレス プールを指定するには、その名前をコマンドに含めます。

ip-phone-bypass

IP Phone Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。IP Phone Bypass をディセーブルにするには、**ip-phone-bypass disable** コマンドを使用します。実行コンフィギュレーションから IP phone Bypass 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションにより、別のグループ ポリシーから IP Phone Bypass の値を継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP フォンが、ユーザ認証プロセスなしで接続できます。イネーブルの場合、セキュア ユニット認証は有効のままになります。

ip-phone-bypass {**enable | disable**}

no ip-phone-bypass

構文の説明

disable	IP Phone Bypass をディセーブルにします。
enable	IP Phone Bypass をイネーブルにします。

デフォルト

IP Phone Bypass はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP Phone Bypass は、ユーザ認証をイネーブルにした場合にだけ設定する必要があります。

例

次に、IP Phone Bypass をイネーブルにする例を示します （FirstGroup というグループ ポリシーに対して）。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

ips

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、AIP SSM をサポートします。これは、プロアクティブでフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなど悪意のあるトラフィックを停止し、ネットワークに影響が及ばないようにします。インスペクションのために適応型セキュリティ アプライアンスから AIP SSM にトラフィックを迂回させるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

構文の説明

fail-close	AIP SSM で障害が発生した場合には、トラフィックをブロックします。
fail-open	AIP SSM で障害が発生しても、トラフィックを許可します。
inline	パケットを AIP SSM に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。
promiscuous	AIP SSM 向けにパケットを複製します。AIP SSM が元のパケットをドロップすることはできません。
sensor {*sensor_name* | *mapped_name*}	このトラフィックの仮想センサー名を設定します。AIP SSM（バージョン 6.0 以降）で仮想センサーを使用する場合は、この引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips ... sensor ?** コマンドを使用します。使用可能なセンサーの一覧が表示されます。また、**show ips** コマンドを使用することもできます。 適応型セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合は、コンテキストに割り当てたセンサーのみを指定できます（**allocate-ips** コマンドを参照）。コンテキストで設定する場合は、*mapped_name* を使用します。 センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。 AIP SSM にまだ存在しない名前を入力した場合は、エラーが発生し、コマンドが拒否されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	仮想センサーのサポートが追加されました。

使用上のガイドライン

適応型セキュリティ アプライアンスに **ips** コマンドを設定する前または後に、AIP SSM にセキュリティ ポリシーを設定します。適応型セキュリティ アプライアンスから AIP SSM へのセッションを確立できるか（**session** コマンド）、または管理インターフェイスで SSH または Telnet を使用して直接 AIP SSM に接続できます。または、ASDM を使用する方法もあります。AIP SSM の設定の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

ips コマンドを設定するには、先に **class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

AIP SSM は、適応型セキュリティ アプライアンスとは別のアプリケーションを実行します。ただし、アプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM には、管理インターフェイス以外に外部インターフェイス自体は含まれていません。適応型セキュリティ アプライアンスでトラフィック クラスに対して **ips** コマンドを適用すると、トラフィックは次のように適応型セキュリティ アプライアンスおよび AIP SSM を経由します。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. トラフィックがバックプレーン経由で AIP SSM に送信されます（**inline** キーワードを使用します。トラフィックのコピーを AIP SSM に送信するだけの場合の詳細については、**promiscuous** キーワードを参照してください）。
4. AIP SSM が、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 有効なトラフィックがバックプレーン経由で適応型セキュリティ アプライアンスに返送されます。AIP SSM が、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが適応型セキュリティ アプライアンスを終了します。

例

次に、無差別モードですべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

次に、インライン モードで 10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生してもすべてのトラフィックを許可する例を示します。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
```

```
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のすべての**ポリシー マップ** コンフィギュレーションを表示します。

ipsec-udp

IPSec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。IPSec over UDP をディセーブルにするには、**ipsec-udp disable** コマンドを使用します。実行コンフィギュレーションから IPSec over UDP 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから IPSec over UDP の値を継承できるようになります。

IPSec through NAT とも呼ばれる IPSec over UDP を使用すると、Cisco VPN Client またはハードウェア クライアントは NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続できます。

ipsec-udp {enable | disable}

no ipsec-udp

構文の説明

disable	IPSec over UDP をディセーブルにします。
enable	IPSec over UDP をイネーブルにします。

デフォルト

IPSec over UDP はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPSec over UDP を使用するには、**ipsec-udp-port** コマンドも設定する必要があります。

さらに、IPSec over UDP を使用するように Cisco VPN Client を設定する必要があります（デフォルトで使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するためのコンフィギュレーションが必要ありません。

IPSec over UDP は独自仕様で、リモート アクセス接続にだけ適用され、モード コンフィギュレーションが必要です。つまり、セキュリティ アプライアンスは SA のネゴシエーション中にクライアントとコンフィギュレーション パラメータを交換します。

IPSec over UDP を使用すると、システム パフォーマンスが若干低下します。

例

次に、FirstGroup というグループ ポリシーの IPSec over UDP を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# ipsec-udp enable
```

関連コマンド

コマンド	説明
ipsec-udp-port	セキュリティ アプライアンスが UDP トラフィックを受信するポートを指定します。

ipsec-udp-port

IPSec over UDP の UDP ポート番号を設定するには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポートをディセーブルにするには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから IPSec over UDP ポートの値を継承できるようになります。

IPSec ネゴシエーションでは、セキュリティ アプライアンスは設定されたポートで待ち受け、他のフィルタ ルールによって UDP トラフィックがドロップされた場合でも、そのポート宛てに UDP トラフィックを転送します。

ipsec-udp-port *port*

no ipsec-udp-port

構文の説明

port	4001 ～ 49151 の範囲内の整数を使用して、UDP ポート番号を識別します。

デフォルト

デフォルトのポートは 10000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この機能をイネーブルにすると、複数のグループ ポリシーを設定し、各グループ ポリシーでそれぞれ別のポート番号を使用できます。

例

次に、FirstGroup というグループ ポリシーの IPSec UDP ポートをポート 4025 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

関連コマンド

コマンド	説明
ipsec-udp	Cisco VPN Client またはハードウェア クライアントは、NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続できるようにします。

ip verify reverse-path

ユニキャスト RPF をイネーブルにするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

構文の説明

interface_name	ユニキャスト RPF をイネーブルにするインターフェイス。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

通常、セキュリティ アプライアンスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるようにセキュリティ アプライアンスに指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。セキュリティ アプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

例

次に、外部インターフェイスでユニキャスト RPF をイネーブルにする例を示します。

```
hostname(config)# ip verify reverse-path interface outside
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

ipv6 access-list

IPv6 アクセス リストを設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リストには、セキュリティ アプライアンスが通過を許可またはブロックするトラフィックを定義します。

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

構文の説明

any	IPv6 プレフィックス ::/0 の省略形で、任意の IPv6 アドレスを示します。
default	（任意）ACE に対して syslog メッセージ 106100 を生成することを指定します。
deny	条件に一致する場合、アクセスを拒否します。
destination-ipv6-address	トラフィックを受信するホストの IPv6 アドレス。
destination-ipv6-prefix	トラフィックの宛先となる IPv6 ネットワーク アドレス。
disable	（任意）syslog メッセージングをディセーブルにします。
host	アドレスが特定のホストを指すよう指定します。
icmp6	セキュリティ アプライアンスを通過する ICMPv6 トラフィックにアクセス ルールを適用することを指定します。

icmp_type	アクセス ルールによってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）、または次の ICMP タイプ リテラルのいずれかを指定できます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect *icmp_type* 引数を省略すると、すべての ICMP タイプを指定したことになります。
icmp_type_obj_grp_id	（任意）オブジェクト グループ ICMP タイプ ID を指定します。
id	アクセス リストの名前または番号。
interval *secs*	（任意）106100 syslog メッセージを生成する時間間隔を指定します。有効な値は、1 ～ 600 秒です。デフォルトの interval は 300 秒です。この値は、非アクティブなフローを削除するためのタイムアウト値としても使用されます。
level	（任意）メッセージ 106100 の syslog レベルを指定します。有効な値は、0 ～ 7 です。デフォルトのレベルは 6（情報）です。
line *line-num*	（任意）アクセス ルールの挿入先となるリスト内の行番号。行番号を指定しなかった場合は、アクセス リストの末尾に ACE が追加されます。
log	（任意）ACE に対するロギング アクションを指定します。**log** キーワードを指定しないか、または **log default** キーワードを指定した場合、ACE によってパケットが拒否されると、メッセージ 106023 が生成されます。log キーワードを単独で指定するか、レベルまたは間隔とともに指定した場合、ACE によってパケットが拒否されると、メッセージ 106100 が生成されます。アクセス リストの末尾にある暗黙的な拒否によって拒否されたパケットは、ログに記録されません。ロギングをイネーブルにするには、ACE で明示的にパケットを拒否する必要があります。
network_obj_grp_id	既存のネットワーク オブジェクト グループ ID。
object-group	（任意）オブジェクト グループを指定します。

operator	（任意）送信元 IP アドレスを宛先 IP アドレスと比較するためのオペランドを指定します。*operator* は、送信元 IP アドレス ポートまたは宛先 IP アドレス ポートを比較するためのものです。有効なオペランドには、より小さいを表す **lt**、より大きいを表す **gt**、一致を表す **eq**、不一致を表す **neq**、包含範囲を表す **range** があります。演算子およびポートを指定せずに **ipv6 access-list** コマンドを使用すると、デフォルトではすべてのポートを指定したことになります。
permit	条件が一致した場合にアクセスを許可します。
port	（任意）アクセスを許可または拒否するポートを指定します。*port* 引数を入力する際、0 ～ 65535 の範囲の番号でポートを指定できます。また、*protocol* が **tcp** または **udp** である場合には、リテラル名を使用できます。 許可される TCP リテラル名は、**aol**、**bgp**、**chargen**、**cifc**、**citrix-ica**、**cmd**、**ctiqbe**、**daytime**、**discard**、**domain**、**echo**、**exec**、**finger**、**ftp**、**ftp-data**、**gopher**、**h323**、**hostname**、**http**、**https**、**ident**、**irc**、**kerberos**、**klogin**、**kshell**、**ldap**、**ldaps**、**login**、**lotusnotes**、**lpd**、**netbios-ssn**、**nntp**、**pop2**、**pop3**、**pptp**、**rsh**、**rtsp**、**smtp**、**sqlnet**、**ssh**、**sunrpc**、**tacacs**、**talk**、**telnet**、**uucp**、**whois**、および **www** です。 許可される UDP リテラル名は、**biff**、**bootpc**、**bootps**、**cifs**、**discard**、**dnsix**、**domain**、**echo**、**http**、**isakmp**、**kerberos**、**mobile-ip**、**nameserver**、**netbios-dgm**、**netbios-ns**、**ntp**、**pcanywhere-status**、**pim-auto-rp**、**radius**、**radius-acct**、**rip**、**secureid-udp**、**snmp**、**snmptrap**、**sunrpc**、**syslog**、**tacacs**、**talk**、**tftp**、**time**、**who**、**www**、および **xdmcp** です。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
protocol	IP プロトコルの名前または番号。有効な値は、**icmp**、**ip**、**tcp**、**udp**、または IP プロトコル番号を表す 1 ～ 254 の範囲の整数です。
protocol_obj_grp_id	既存のプロトコル オブジェクト グループ ID。
service_obj_grp_id	（任意）オブジェクト グループを指定します。
source-ipv6-address	トラフィックを送信するホストの IPv6 アドレス。
source-ipv6-prefix	ネットワーク トラフィックの送信元である IPv6 ネットワーク アドレス。

デフォルト

log キーワードを指定した場合、syslog メッセージ 106100 のデフォルト レベルは 6（情報）です。

デフォルトのロギング間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 access-list コマンドを使用すると、IPv6 アドレスにポートまたはプロトコルへのアクセスを許可するのか拒否するのかを指定できます。各コマンドは ACE と呼ばれます。同じアクセス リスト名を持つ 1 つまたは複数の ACE はアクセス リストと呼ばれます。**access-group** コマンドを使用して、インターフェイスにアクセス リストを適用します。

セキュリティ アプライアンスは、アクセス リストを使用して明示的にアクセスを許可しない限り、外部インターフェイスから内部インターフェイスへのパケットをすべて拒否します。内部インターフェイスから外部インターフェイスへのパケットは、明示的にアクセスを拒否しない限り、デフォルトですべて許可されます。

ipv6 access-list コマンドは、IPv6 固有である点を除いて、**access-list** コマンドに似ています。アクセス リストの詳細については、**access-list extended** コマンドを参照してください。

ipv6 access-list icmp コマンドは、セキュリティ アプライアンスを通過する ICMPv6 メッセージをフィルタリングするために使用されます。特定のインターフェイスでの発信および終端が許可される ICMPv6 トラフィックを設定するには、**ipv6 icmp** コマンドを使用します。

オブジェクト グループを設定する方法については、**object-group** コマンドを参照してください。

例

次に、ホストが TCP を使用して 3001:1::203:A0FF:FED6:162D サーバにアクセスできるようにする例を示します。

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
```

次の例では、**eq** とポートを使用して、FTP へのアクセスだけを拒否します。

```
hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp
hostname(config)# access-group acl_out in interface inside
```

次の例では、**lt** を使用して、2025 より小さいすべてのポートへのアクセスを許可します。これにより、予約済みポート（1 ～ 1024）へのアクセスが許可されます。

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host 3001:1::203:A0FF:FED6:162D
lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスに割り当てます。
ipv6 icmp	セキュリティ アプライアンスのインターフェイスで終了する ICMP メッセージに対するアクセス ルールを設定します。
object-group	オブジェクト グループ（アドレス、ICMP タイプ、およびサービス）を作成します。

ipv6 access-list webtype

クライアントレス SSL VPN に対するフィルタリングをサポートする設定に追加できる IPv6 アクセス リストを作成するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用し、構文ストリング全体をコンフィギュレーションにあるとおりに指定します。

ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

no ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

構文の説明

id	アクセス リストの名前または番号。
any	すべての対象へのアクセスを指定します。
deny	条件に一致する場合、アクセスを拒否します。
permit	条件に合致している場合、アクセスを許可します。
url	フィルタリングに URL を使用することを指定します。
url_string	（任意）フィルタリングする URL を指定します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

次のワイルドカード文字を使用すると、Webtype アクセス リスト エントリに複数のワイルドカードを定義できます。

- 0 個以上の任意の数の文字に一致させるには、アスタリスク「*」を入力します。
- 任意の 1 文字に正確に一致させるには、疑問符「?」を入力します。
- 範囲内の任意の 1 文字に一致する範囲演算子を作成するには、角カッコ「[ ]」を入力します。

例

この項の例では、IPv6 Webtype アクセス リストでのワイルドカードの使用方法を示します。

- 次に、http://www.cisco.com/ や http://wwz.caco.com/ などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url http://ww?.c*co*/
```

- 次に、http://www.cisco.com や ftp://wwz.carrier.com などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url *://ww?.c*co*/
```

- 次の例は、http://www.cisco.com:80 や https://www.cisco.com:81 などの URL に一致します。

```
ipv6 access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上記の例に示した range 演算子「[]」は、文字 0 または 1 が出現可能であることを指定します。

- 次に、http://www.google.com や http://www.boogie.com などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url http://www.[a-z]oo?*/
```

上記の例に示した range 演算子「[]」は、a ～ z の範囲内の任意の 1 文字が出現可能であることを指定します。

- 次の例は、http://www.cisco.com/anything/crazy/url/ddtscgiz などの URL に一致します。

```
ipv6 access-list test webtype permit url htt*://*/*cgi?*
```

（注） 任意の http URL に一致させるには、http://* を入力するというこれまでの方法ではなく、http://*/* を入力する必要があります。

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
show running-config access-list	適応型セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

ipv6 address

IPv6 をイネーブルにし、インターフェイス上で IPv6 アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

no ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

構文の説明

autoconfig	インターフェイスでステートレス自動設定を使用して、IPv6 アドレスの自動設定をイネーブルにします。
eui-64	（任意）IPv6 アドレスの下位 64 ビットにインターフェイス ID を指定します。
ipv6-address	インターフェイスに割り当てられた IPv6 リンクローカル アドレス。
ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク アドレス。
link-local	アドレスがリンクローカル アドレスであることを指定します。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスに IPv6 アドレスを設定すると、そのインターフェイスで IPv6 がイネーブルになります。IPv6 アドレスを指定した後で **ipv6 enable** コマンドを使用する必要はありません。

ipv6 address autoconfig コマンドは、ステートレス自動設定を使用してインターフェイスで IPv6 アドレスの自動設定をイネーブルにするために使用されます。アドレスは、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて設定されます。リンクローカル アドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。別のホストがリンクローカル アドレスを使用している場合には、エラー メッセージが表示されます。

ipv6 address eui-64 コマンドは、インターフェイスの IPv6 アドレスを設定するために使用されます。任意の **eui-64** を指定した場合、アドレスの下位 64 ビットに EUI-64 インターフェイス ID が使用されます。*prefix-length* 引数に指定されている値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

ipv6 address link-local コマンドは、インターフェイスの IPv6 リンクローカル アドレスを設定するために使用されます。このコマンドに指定された *ipv6-address* は、インターフェイス用に自動的に生成されるリンクローカル アドレスを上書きします。リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。MAC アドレスが 00E0.B601.3B7A のインターフェイスの場合、リンクローカル アドレスは FE80::2E0:B6FF:FE01:3B7A になります。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

例

次に、選択したインターフェイスのグローバル アドレスとして 3FFE:C00:0:1::576/64 を割り当てる例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

次に、選択したインターフェイスに自動的に IPv6 アドレスを割り当てる例を示します。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

次の例では、選択したインターフェイスに IPv6 アドレス 3FFE:C00:0:1::/64 を割り当て、アドバイザーの下位 64 ビットに EUI-64 インターフェイス ID を指定します。

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

次に、選択したインターフェイスのリンク レベル アドレスとして FE80::260:3EFF:FE11:6670 を割り当てる例を示します。

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

関連コマンド

コマンド	説明
debug ipv6 interface	IPv6 インターフェイスのデバッグ情報を表示します。
show ipv6 interface	IPv6 用に設定されたインターフェイスのステータスを表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable

no ipv6 enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイスに IPv6 リンクローカル ユニキャスト アドレスを自動的に設定し、さらにインターフェイスを IPv6 処理用にイネーブルにします。

明示的な IPv6 アドレスで設定されているインターフェイスで **no ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

次に、選択したインターフェイスで IPv6 処理をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスの IPv6 アドレスを設定し、インターフェイス上で IPv6 の処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 enforce-eui64

ローカル リンク上の IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用するには、グローバル コンフィギュレーション モードで **ipv6 enforce-eui64** コマンドを使用します。Modified EUI-64 アドレス形式の適用をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

構文の説明

if_name	Modified EUI-64 アドレス形式の適用をイネーブルにするインターフェイスの名前を **nameif** コマンドで指定されているとおりに指定します。

デフォルト

Modified EUI-64 形式の適用はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドがインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

48 ビット リンク層（MAC）アドレスから Modified EUI-64 形式のインターフェイス ID を取得するには、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）との間に 16 進数 FFFE を挿入します。選択されたアドレスが一意のイーサネット MAC アドレスから生成され

ることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

例

次に、内部インターフェイスで受信した IPv6 アドレスに対して Modified EUI-64 形式の適用をイネーブルにする例を示します。

```
hostname(config)# ipv6 enforce-eui64 inside
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスで IPv6 アドレスを設定します。
ipv6 enable	インターフェイス上で IPv6 をイネーブルにします。

ipv6 icmp

インターフェイスの ICMP アクセス ルールを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp** コマンドを使用します。ICMP アクセス ルールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

構文の説明

any	IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の省略形。
deny	選択したインターフェイスで指定の ICMP トラフィックを阻止します。
host	アドレスが特定のホストを指すよう指定します。
icmp-type	アクセス ルールによってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）、または次の ICMP タイプ リテラルのいずれかを指定できます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	アクセス ルールが適用されるインターフェイスの名前（**nameif** コマンドで指定した名前）。
ipv6-address	ICMPv6 メッセージをインターフェイスに送信しているホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信している IPv6 ネットワーク。
permit	選択したインターフェイスで指定の ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。

デフォルト

ICMP アクセス ルールが定義されていない場合、すべての ICMP トラフィックが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 の ICMP は、IPv4 の ICMP と同じ働きをします。ICMPv6 によって、ICMP 宛先到達不能メッセージなどのエラー メッセージや、ICMP エコー要求および応答メッセージのような情報メッセージが生成されます。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索プロセスおよびパス MTU ディスカバリに使用されます。

インターフェイスに対して定義されている ICMP ルールがない場合、すべての IPv6 ICMP トラフィックが許可されます。

インターフェイスに対して定義されている ICMP ルールが複数ある場合は、最初に一致したルールから順に処理され、その後暗黙のすべて拒否ルールが続きます。たとえば、最初に一致したルールが許可ルールである場合、ICMP パケットは処理されます。最初に一致したルールが拒否ルールである場合、または ICMP パケットがそのインターフェイスのどのルールにも一致しなかった場合、セキュリティ アプライアンスは ICMP パケットを廃棄し、syslog メッセージを生成します。

そのため、ICMP ルールを入力する順序が重要になります。特定のネットワークからの ICMP トラフィックをすべて拒否するルールを入力し、その後にそのネットワーク上の特定のホストからの ICMP トラフィックを許可するルールが続く場合、ホストのルールはいっさい処理されません。ICMP トラフィックは、ネットワークのルールによってブロックされます。ただし、ホストのルールを先に入力し、その後にネットワークのルールを続けた場合、そのホストからの ICMP トラフィックは許可され、そのネットワークからのそれ以外の ICMP トラフィックはブロックされます。

ipv6 icmp コマンドは、セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。パススルー ICMP トラフィックのアクセス ルールを設定するには、**ipv6 access-list** コマンドを参照してください。

例

次に、外部インターフェイスですべての ping 要求を拒否し、（パス MTU ディスカバリをサポートするため）すべての Packet Too Big メッセージを許可する例を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次に、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する例を示します。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

関連コマンド

コマンド	説明
ipv6 access-list	アクセス リストを設定します。

ipv6 local pool

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 local pool** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

no ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

構文の説明

pool_name	この IPv6 アドレス プールに割り当てる名前を指定します。
ipv6_address	設定する IPv6 アドレス プールを指定します。形式は x:x:x:: です。
number_of_addresses	範囲：1 ～ 16384
prefix_length	範囲：0 ～ 128

デフォルト

デフォルトでは、IPv6 ローカル アドレス プールは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

IPv6 ローカル プールを割り当てるには、トンネル グループで **ipv6-local-pool** コマンドを使用するか、またはグループ ポリシーで **ipv6-address-pools**（末尾の「s」に注意）コマンドを使用します。グループ ポリシーの ipv6-address-pools 設定は、トンネル グループの ipv6-address-pool 設定を上書きします。

例

次に、設定一般コンフィギュレーション モードを開始し、アドレスをリモート クライアントに割り当てるために使用される IPv6 アドレス プールを firstipv6pool という名前で設定する例を示します。

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
hostname(config)#
```

関連コマンド

コマンド	説明
ipv6-address-pool	IPv6 アドレス プールを VPN トンネル グループ ポリシーに関連付けます。
ipv6-address-pools	IPv6 アドレス プールを VPN グループ ポリシーに関連付けます。
clear configure ipv6 local pool	設定済みのすべての IPv6 ローカル プールをクリアします。
show running-config ipv6	IPv6 のコンフィギュレーションを表示します。

ipv6 nd dad attempts

重複アドレス検出時にインターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信する重複アドレス検出メッセージの数をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

構文の説明

value	0 ～ 600 までの数字。0 を入力すると、指定したインターフェイスでの重複アドレス検出がディセーブルになります。1 を入力すると、後続の送信なしの単一の送信が設定されます。デフォルト値は 1 メッセージです。

デフォルト

デフォルトの試行回数は 1 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。ネイバー送信要求メッセージの送信頻度を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。

インターフェイスが管理上アップ状態に戻ると、そのインターフェイスで重複アドレス検出が自動的に再起動されます。管理上アップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスを対象に重複アドレス検出が再起動されます。

（注）　インターフェイスのリンクローカル アドレスで重複アドレス検出が実行されている間、他の IPv6 アドレスの状態は仮承諾に設定されたままとなります。リンクローカル アドレスで重複アドレス検出が完了すると、残りの IPv6 アドレスで重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

重複アドレスがインターフェイスのグローバル アドレスである場合、そのアドレスは使用されず、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

アドレスの状態が DUPLICATE に設定されている間、重複アドレスに関連付けられたコンフィギュレーション コマンドはすべて設定済みのままとなります。

インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカル アドレスでのみ実行されます）。

例

次に、重複アドレス検出がインターフェイスの仮承諾のユニキャスト IPv6 アドレスで実行された場合に、5 つ連続して送信されるネイバー送信要求メッセージを設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

次に、選択したインターフェイスで重複アドレス検出をディセーブルにする例を示します。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイスで IPv6 ネイバー送信要求メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ns-interval

インターフェイスで IPv6 ネイバー送信要求メッセージが再送信される時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

構文の説明

value	IPv6 ネイバー送信要求メッセージが送信される時間間隔（ミリ秒単位）。有効な値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

デフォルト

ネイバー送信要求メッセージが送信される時間間隔は 1000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

例

次に、GigabitEthernet 0/0 の IPv6 ネイバー送信要求送信間隔を 9000 ミリ秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd prefix

IPv6 ルータ アドバタイズメントにどの IPv6 プレフィックスを含めるかを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

構文の説明

at *valid-date preferred-date*	ライフタイムおよびプリファレンスが期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表されます。
default	デフォルト値が使用されます。
infinite	（任意）有効なライフタイムが期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
no-advertise	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。
no-autoconfig	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用できないことを示します。
off-link	（任意）指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる時間（秒単位）。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは infinite を使用して指定もできます。デフォルトは 604800（7 日間）です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
valid-lifetime	指定された IPv6 プレフィックスが有効プレフィックスとしてアドバタイズされる時間。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限を表します。**infinite** として指定することもできます。デフォルトは、2592000（30 日）です。

デフォルト

IPv6 ルータ アドバタイズメントを発信するインターフェイスに設定されているすべてのプレフィックスが、有効ライフタイム 2592000 秒（30 日）および優先ライフタイム 604800 秒（7 日）でアドバタイズされます。どちらのライフタイムにも「onlink」フラグと「autoconfig」フラグが設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに個々のパラメータを制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメント用にプレフィックスを設定した場合は、そのプレフィックスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィックスのデフォルト パラメータを設定できます。

プレフィックスの有効期限を指定するための日付を設定できます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。有効期限に達すると、プレフィックスはアドバタイズされなくなります。

onlink が「on」（デフォルト）である場合、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

autoconfig が「on」（デフォルト）である場合、ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用できることを示します。

例

次に、有効ライフタイムを 1000 秒、優先ライフタイムを 900 秒にして、指定したインターフェイスから送信されるルータ アドバタイズメントに IPv6 プレフィックス 2001:200::/35 を含める例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	IPv6 アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-interval

インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

構文の説明

msec	（任意）指定される値がミリ秒単位であることを示します。このキーワードが指定されていない場合、指定される値は秒単位となります。
value	IPv6 ルータ アドバタイズメントの送信間隔。有効な値の範囲は、3 ～ 1800 秒であるか、**msec** キーワードが指定されている場合には 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

デフォルト

200 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 nd ra-lifetime コマンドを使用してセキュリティ アプライアンスがデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20 % 以内でランダムに調整します。

例

次に、選択したインターフェイスで IPv6 ルータ アドバタイズメントの間隔を 201 秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-lifetime

インターフェイス上で IPv6 ルータ アドバタイズメントに「ルータ ライフタイム」値を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

構文の説明

seconds	セキュリティ アプライアンスがこのインターフェイスでデフォルト ルータであることの有効性。有効な値の範囲は、0 ～ 9000 秒です。デフォルトは 1,800 秒です。0 は、セキュリティ アプライアンスを、選択したインターフェイス上のデフォルト ルータと見なしてはならないことを示します。

デフォルト

1800 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

「ルータ ライフタイム」値は、インターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。値は、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータとして有効であることを示します。

値をゼロ以外の値に設定すると、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータであると見なされます。「ルータ ライフタイム」値をゼロ以外の値にする場合、ルータ アドバタイズメント間隔を下回る値にはしないでください。

値を 0 に設定すると、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータであると見なされません。

例

次に、選択したインターフェイス上で IPv6 ルータ アドバタイズメントのライフタイムを 1801 秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイスで IPv6 Router Advertisement（RA; ルータ アドバタイズメント）メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd reachable-time

到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

構文の説明

value	リモート IPv6 ノードが到達可能であると見なされる時間（ミリ秒単位）。有効な値の範囲は、0 ～ 3600000 ミリ秒です。デフォルト値は 0 です *value* に 0 を使用すると、到達可能時間が未定のまま送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

デフォルト

0 ミリ秒

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間を設定すると、使用不可能なネイバーの検出がイネーブルになります。設定時間を短くすると、使用不可能なネイバーをさらに迅速に検出できます。ただし、時間を短くすると、すべての IPv6 ネットワーク デバイスで IPv6 ネットワーク帯域幅および処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

このコマンドが 0 に設定されている際の実際の値を含め、セキュリティ アプライアンスで使用されている到達可能時間を参照するには、**show ipv6 interface** コマンドを使用して、使用されている ND 到達可能時間など IPv6 インターフェイスに関する情報を表示します。

例

次に、選択したインターフェイスで IPv6 到達可能時間を 1700000 ミリ秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd suppress-ra

LAN インターフェイスで IPv6 ルータ アドバタイズメントの送信を抑制するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスで IPv6 ルータ アドバタイズメントの送信を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IPv6 ユニキャスト ルーティングがイネーブルになっている場合、ルータ アドバタイズメントは LAN インターフェイスで自動的に送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LAN 以外のインターフェイス タイプ（たとえばシリアル インターフェイスやトンネル インターフェイス）で IPv6 ルータ アドバタイズメントの送信をイネーブルにするには、**no ipv6 nd suppress-ra** コマンドを使用します。

例

次に、選択したインターフェイスで IPv6 ルータ アドバタイズメントを抑制する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 neighbor

IPv6 ネイバー探索キャッシュにスタティック エントリを設定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor** コマンドを使用します。ネイバー探索キャッシュからスタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

構文の説明

if_name	**nameif** コマンドで指定された内部インターフェイス名または外部インターフェイス名。
ipv6_address	ローカル データリンク アドレスに対応する IPv6 アドレス。
mac_address	ローカル データ回線（ハードウェア MAC）アドレス。

デフォルト

スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 neighbor コマンドは、**arp** コマンドに似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、**copy** コマンドを使用してコンフィギュレーションを格納すると、コンフィギュレーションに格納されます。

IPv6 ネイバー探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。

clear ipv6 neighbors コマンドは、スタティック エントリを除いて IPv6 ネイバー探索キャッシュのすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、ネイバー探索キャッシュから指定のスタティック エントリを削除します。ダイナミック エントリ（IPv6 ネイバー探索プロセスから学習したエントリ）はキャッシュから削除されません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

例

次に、IPv6 アドレスを 3001:1::45A、MAC アドレスを 0002.7D1A.9472 にして、内部ホスト用のスタティック エントリをネイバー探索キャッシュに追加する例を示します。

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

ipv6 route

IPv6 ルートを IPv6 ルーティング テーブルに追加するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。IPv6 デフォルト ルートを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

no ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

構文の説明

administrative-distance	（任意）ルートのアドミニストレーティブ ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは接続ルートを除く他のどのタイプのルートよりも優先されます。
if_name	ルートが設定されているインターフェイスの名前。
ipv6-address	指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
tunneled	（任意）ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

デフォルトでは、*administrative-distance* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 ルーティング テーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

tunneled オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

例

次に、アドミニストレーティブ ディスタンスを 110 にして、ネットワーク 7fff::0/32 のパケットを 3FFE:1100:0:CC00::1 にある内部インターフェイス上のネットワーキング デバイスにルーティングする例を示します。

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブル アップデートおよびルート キャッシュ アップデートのデバッグ メッセージを表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

ipv6-address-pool（トンネル グループ一般属性モード）

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **ipv6-address-pool** コマンドを使用します。IPv6 アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

構文の説明

ipv6_address_pool	**ipv6 local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface_name	（任意）アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **ipv6-address-pools** コマンドの IPv6 アドレス プール設定は、トンネル グループの **ipv6-address-pool** コマンドの IPv6 アドレス プール設定を上書きします。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードを開始し、IPSec リモート アクセス トンネル グループ テスト用に、アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定する例を示します。

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general-attributes
```

```
hostname(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ipv6-address-pools	グループ ポリシーの IPv6 アドレス プール設定を設定します。これらの設定は、トンネル グループの IPv6 アドレス プール設定を上書きします。
ipv6 local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group	トンネル グループを設定します。

ipv6-address-pools

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを最大 6 つ指定するには、グループ ポリシー属性コンフィギュレーション モードで **ipv6-address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

ipv6-address-pools none

no ipv6-address-pools none

構文の説明

ipv6_address_pool	**ipv6 local pool** コマンドで設定した最大 6 つの IPv6 アドレス プールの名前を指定します。各 IPv6 アドレス プール名を区切るには、スペースを使用します。
none	IPv6 アドレス プールが設定されず、他のグループ ポリシーからの継承をディセーブルにすることを指定します。
value	アドレスを割り当てるための IPv6 アドレス プールを最大 6 つ指定します。

デフォルト

デフォルトでは、IPv6 アドレス プールの属性は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

IPv6 アドレス プールを設定するには、**ipv6 local pool** コマンドを使用します。

ipv6-address-pools コマンドにプールを指定する順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

ipv6-address-pools none コマンドは、この属性が DefaultGrpPolicy など他のポリシーから継承されることをディセーブルにします。**no ipv6-address-pools none** コマンドは、コンフィギュレーションから **ipv6--address-pools none** コマンドを削除して、デフォルト値に戻します。これにより、継承が許可されます。

例

次に、設定一般コンフィギュレーション モードを開始し、アドレスをリモート クライアントに割り当てるために使用される IPv6 アドレス プールを firstipv6pool という名前で設定し、そのプールを GroupPolicy1 に関連付ける例を示します。

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# ipv6-address-pools value firstipv6pool
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
ipv6 local pool	VPN グループ ポリシーに使用される IPv6 アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

ipv6-vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グループ ポリシー モードまたはユーザ名モードで **ipv6-vpn-filter** コマンドを使用します。**ipv6-vpn-filter none** コマンドの発行によって作成されるヌル値を含め、ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値の継承を防止するには、**ipv6-vpn-filter none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**ipv6-vpn-filter** コマンドを使用して、その ACL を適用します。

ipv6-vpn-filter {**value** *IPV6-ACL-NAME* | **none**}

no ipv6-vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *IPV6-ACL-NAME*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

クライアントレス SSL VPN は、**ipv6-vpn-filter** コマンドに定義されている ACL を使用しません。

例

次に、FirstGroup というグループ ポリシーの ipv6_acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-vpn-filter value ipv6_acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。

isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

isakmp am-disable

no isakmp am-disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp am-disable** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
hostname(config)# isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp disconnect-notify

ピアへの切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp disconnect-notify

no isakmp disconnect-notify

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp disconnect-notify** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信しているインターフェイスで ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。インターフェイスで ISAKMP をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp enable *interface-name*

no isakmp enable *interface-name*

構文の説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp enable** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp identity

ピアに送信されるフェーズ 2 ID を設定するには、グローバル コンフィギュレーション モードで **isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	接続タイプによって ISKMP ネゴシエーションを決定します。事前共有キーの場合は IP アドレス、証明書認証の場合は証明書 DN となります。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

デフォルト

デフォルトの ISAKMP の識別情報は、**isakmp identity hostname** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp identity** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

```
hostname(config)# isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp ikev1-user-authentication

IKE 時にハイブリッド認証を設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **isakmp ikev1-user-authentication** コマンドを使用します。ハイブリッド認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

構文の説明

hybrid	IKE 時にハイブリッド XAUTH 認証を指定します。
interface	（任意）ユーザ認証方式が設定されているインターフェイスを指定します。
none	IKE 時にユーザ認証をディセーブルにします。
xauth	拡張ユーザ認証とも呼ばれる XAUTH を指定します。

デフォルト

デフォルトの認証方式は XAUTH、つまり拡張ユーザ認証です。デフォルトの *interface* は、すべてのインターフェイスです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンス認証にデジタル証明書を使用し、リモート VPN ユーザ認証に RADIUS、TACACS+、SecurID などの別の従来の方式を使用する必要がある場合に使用します。このコマンドは、IKE のフェーズ 1 をハイブリッド認証と呼ばれる次の 2 つの手順に分けます。

1. セキュリティ アプライアンスは、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
2. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

任意の **interface** パラメータを省略すると、コマンドはすべてのインターフェイスに適用され、インターフェイスごとのコマンドが指定されていないときにはバックアップとなります。トンネル グループに指定されている **isakmp ikev1-user-authentication** コマンドが 2 つある場合、1 つは **interface** パラメータを使用し、もう 1 つは使用しません。インターフェイスを指定している方が、その特定のインターフェイスでは優先されます。

例

次に、example-group というトンネル グループの内部インターフェイスでハイブリッド XAUTH をイネーブルにする例を示します。

```
hostname(config)# tunnel-group example-group type ipsec-ra
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバを定義します。
pre-shared-key	IKE 接続をサポートするための事前共有キーを作成します。
tunnel-group	IPSec、L2TP/IPSec、および WebVPN 接続の接続固有レコードのデータベースを作成および管理します。

isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	（任意）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp ipsec-over-tcp** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、IPSec over TCP をポート 45 でイネーブルにします。

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp keepalive

IKE DPD を設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **isakmp keepalive** コマンドを使用します。あらゆるトンネル グループで、IKE キープアライブがデフォルトでイネーブルであり、しきい値と再試行値がデフォルト値になっています。キープアライブ パラメータをデフォルトのしきい値と再試行値でイネーブルの状態に戻すには、このコマンドの **no** 形式を使用します。

isakmp keepalive [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

no isakmp keepalive disable

構文の説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
retry *seconds*	キープアライブ応答を受信しなかったことを受けて再試行する間隔を秒単位で指定します。指定できる範囲は 2 ～ 10 秒です。デフォルトは 2 秒です。
threshold *seconds*	キープアライブ モニタリングを開始せずにピアがアイドル状態でいられる秒数を指定します。範囲は 10 ～ 3600 秒です。デフォルトは、LAN-to-LAN グループでは 10 秒、リモート アクセス グループでは 300 秒です。

デフォルト

リモート アクセス グループのデフォルトは、しきい値が 300 秒、再試行値が 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒、再試行値が 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス タイプおよび IPSec LAN-to-LAN トンネル グループ タイプにのみ適用できます。

例

次に、設定 ipsec コンフィギュレーション モードを開始し、IP アドレスが 209.165.200.225 の IPSec LAN-to-LAN トンネル グループに対して、IKE DPD を設定し、しきい値を 15 にし、再試行間隔を 10 に指定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
```

```
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

isakmp nat-traversal

NAT トラバーサルをグローバルにイネーブルにするには、ISAKMP がグローバル コンフィギュレーション モードでイネーブルになっていることを確認し（**isakmp enable** コマンドでイネーブルにできます）、次に **isakmp nat-traversal** コマンドを使用します。NAT トラバーサルをイネーブルにした場合、このコマンドの **no** 形式でディセーブルにできます。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトでは、NAT トラバーサル（**isakmp nat-traversal**）はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドは、それに置き換わるものです。

使用上のガイドライン

ポート アドレス変換（PAT）を含めネットワーク アドレス変換（NAT）は、IPSec が使用されているものの、IPSec パケットの NAT デバイス通過を阻害する非互換性がいくつもあるネットワークの多くで使用されています。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは IETF のドラフト「UDP Encapsulation of IPsec Packets」のバージョン 2 およびバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に従って NAT トラバーサルをサポートし、NAT トラバーサルはダイナミック クリプト マップとスタティック クリプト マップの両方に対応しています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次の例では、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、30 秒間隔で NAT Traversal をイネーブルにします。

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy authentication

IKE ポリシー内に認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

構文の説明

crack	認証方式として IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。7.0 で DSA-Sig が追加されました。

使用上のガイドライン

RSA シグニチャを指定した場合、Certification Authority（CA; 認証局）から証明書を取得するように、セキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy authentication** コマンドを使用する例を示します。この例では、使用する RSA シグニチャの認証方式を IKE ポリシー内にプライオリティ番号 40 で設定します。

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy encryption

使用する暗号化アルゴリズムを IKE ポリシー内に指定するには、グローバル コンフィギュレーション モードで **isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy encryption** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy encryption** コマンドを使用する例を示します。使用するアルゴリズムとして 128 ビット キー AES 暗号化を IKE ポリシー内にプライオリティ番号 25 で設定します。

```
hostname(config)# isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
hostname(config)# isakmp policy 40 encryption 3des
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **group** {**1 | 2 | 5**}

no isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトはグループ 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。グループ 7 が追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy group** コマンドは、それに置き換わるものです。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注）　Cisco VPN Client バージョン 3.x 以降で DH **グループ 2** を設定するには、**isakmp policy** が必要です（DH **グループ 1** を設定した場合、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）**グループ 1** や**グループ 2** ではなく、**グループ 5** を使用する必要があります。このためには、**isakmp policy priority group 5** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

```
hostname(config)# isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **hash** {**md5 | sha**}

no isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーでハッシュ アルゴリズムとして MD5（HMAC バリアント）を使用することを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーでハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を使用することを指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy hash** コマンドは、それに置き換わるものです。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

例

次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy hash** コマンドを使用する例を示します。この例では、MD5 ハッシュ アルゴリズムを IKE ポリシー内でプライオリティ番号 40 で使用することを指定します。

```
hostname(config)# isakmp policy 40 hash md5
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy lifetime

期限切れになるまでの IKE セキュリティ アソシエーションのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

構文の説明

priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドは、それに置き換わるものです。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルト値の採用を推奨しますが、ピアがライフタイムを提示しない場合には、無限のライフタイムを指定できます。

（注）　IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。
次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy lifetime** コマンドを使用する例を示します。この例では、IKE ポリシー内にプライオリティ番号 40 で IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

例

次に、グローバル コンフィギュレーション モードを開始し、IKE ポリシー内にプライオリティ番号 40 で IKE セキュリティ アソシエーションのライフタイムを 50,4000 秒（14 時間）を設定する例を示します。

```
hostname(config)# isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
hostname(config)# isakmp policy 40 lifetime 0
```

関連コマンド

clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp reload-wait

すべてのアクティブなセッションが自主的に終了するまで待機してからセキュリティ アプライアンスをリブートできるようにするには、グローバル コンフィギュレーション モードで **isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずにセキュリティ アプライアンスをリブートするには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp reload-wait** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからセキュリティ アプライアンスをリブートするように設定します。

```
hostname(config)# isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

issuer

アサーションを SAML-type SSO サーバに送信するセキュリティ デバイスを指定するには、その特定の SAML タイプの webvpn-sso-saml コンフィギュレーション モードで **issuer** コマンドを使用します。発行者名を削除するには、このコマンドの **no** 形式を使用します。

issuer *identifier*

no issuer [*identifier*]

構文の説明

identifier	セキュリティ デバイス名を指定します。通常は、デバイスのホスト名です。識別情報は、英数字で 65 文字未満にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn-sso-saml コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

例

次に、asa1.mycompany.com というセキュリティ デバイスの発行者名を指定する例を示します。

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# issuer asa1.example.com
hostname(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
assertion-consumer-url	セキュリティ デバイスが SAML-type SSO サーバ アサーション コンシューマ サービスに問い合わせる際に使用する URL を指定します。

コマンド	説明
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

issuer-name

すべての発行済み証明書の発行者名 DN を指定するには、ローカル Certificate Authority（CA; 認証局）サーバ コンフィギュレーション モードで **issuer-name** コマンドを使用します。認証局の証明書からサブジェクト DN を削除するには、このコマンドの **no** 形式を使用します。

issuer-name *DN-string*

no issuer-name [*DN-string*]

構文の説明

DN-string	自己署名 CA 証明書のサブジェクト名 DN でもある証明書の認定者名を指定します。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。発行者名は、英数字で 500 文字未満にする必要があります。

デフォルト

デフォルトの発行者名は cn=*hostame.domain-name* で、たとえば cn=asa.example.com となります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(1)	このコマンドが導入されました。
8.0(2)	*DN-string* 値でカンマを保持するため、引用符のサポートが追加されました。

使用上のガイドライン

このコマンドでは、このローカル CA サーバが作成する証明書に表示される発行者名を指定します。この任意のコマンドは、発行者名をデフォルトの CA 名とは異なるものにする場合に使用します。

（注） この発行者名コンフィギュレーションは、いったん CA サーバをイネーブルにし、**no shutdown** コマンドを発行して証明書を生成すると変更できなくなります。

例

次に、証明書認証を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco
systems, inc."
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
keysize	証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA の特性を表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。

CHAPTER 17

java-trustpoint コマンド～ kill コマンド

java-trustpoint

指定したトラストポイントの場所から PKCS12 証明書とキー関連情報を使用するように WebVPN Java オブジェクト署名機能を設定するには、Webvpn コンフィギュレーション モードで **java-trustpoint** コマンドを使用します。

Java オブジェクト署名のトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

java-trustpoint *trustpoint*

no java-trustpoint

構文の説明

trustpoint	**crypto ca import** コマンドによって設定されたトラストポイントの場所を指定します。

デフォルト

デフォルトでは、Java オブジェクト署名のトラストポイントは none に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(2)	このコマンドが導入されました。

使用上のガイドライン

トラストポイントは、Certificate Authority（CA; 認証局）または ID キー ペアを表します。java-trustpoint コマンドの場合、指定したトラストポイントにはアプリケーション署名エンティティの X.509 証明書、その証明書に対応する RSA 秘密キー、ルート CA までの認証局チェーンを含める必要があります。そのためには通常、**crypto ca import** コマンドを使用して PKCS12 形式のバンドルをインポートします。PKCS12 バンドルは、信頼できる CA 認証局から入手するか、openssl といったオープン ソース ツールを使用して既存の X.509 証明書と RSA 秘密キーから手動で作成できます。

例

次に、最初に新しいトラストポイントを設定してから、そのトラストポイントを WebVPN Java オブジェクト署名用に設定する例を示します。次のコマンドは、mytrustpoint という新しいトラストポイントを作成します。

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)#
```

次に、WebVPN Java オブジェクトに署名する新しいトラストポイントを設定する例を示します。

```
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca import	PKCS12 データを使用してトラストポイントの証明書とキーペアをインポートします。

join-failover-group

コンテキストをフェールオーバー グループに割り当てるには、コンテキスト コンフィギュレーション モードで **join-failover-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

join-failover-group *group_num*

no join-failover-group *group_num*

構文の説明

group_num	フェールオーバー グループの番号を指定します。

デフォルト

フェールオーバー グループ 1。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

管理コンテキストは、常にフェールオーバー グループ 1 に割り当てられます。フェールオーバー グループとコンテキスト アソシエーションを表示するには、**show context detail** コマンドを使用できます。

コンテキストをフェールオーバー グループに割り当てる前に、**failover group** コマンドを使用して、フェールオーバー グループをシステム コンテキスト内に作成する必要があります。このコマンドは、コンテキストがアクティブ状態になっているユニット上で入力します。デフォルトでは、未割り当てのコンテキストは、フェールオーバー グループ 1 のメンバーになっています。そのため、コンテキストがまだフェールオーバー グループに割り当てられていない場合は、フェールオーバー グループ 1 がアクティブ状態になっているユニット上で、このコマンドを入力する必要があります。

システムからフェールオーバー グループを削除するには、事前に **no join-failover-group** コマンドを使用して、フェールオーバー グループからコンテキストをすべて削除しておく必要があります。

例

次に、ctx1 というコンテキストをフェールオーバー グループ 2 に割り当てる例を示します。

```
hostname(config)# context ctx1
hostname(config-context)# join-failover-group 2
hostname(config-context)# exit
```

関連コマンド

コマンド	説明
context	指定したコンテキストのコンテキスト コンフィギュレーション モードを開始します。
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
show context detail	コンテキストの詳細情報（名前、クラス、インターフェイス、フェールオーバー グループ アソシエーション、およびコンフィギュレーション ファイルの URL など）を表示します。

keepout

セキュリティ アプライアンスのメンテナンスまたはトラブルシューティングの実施時に、新しいユーザ セッションのログイン ページではなく、立ち入り禁止の Web ページを表示するには、webvpn コンフィギュレーション モードで **keepout** コマンドを使用します。過去に設定した立ち入り禁止ページを削除するには、このコマンドの **no** バージョンを使用します。

keepout

no keepout *string*

構文の説明

string	二重引用符で囲んだ英数字ストリング。

デフォルト

立ち入り禁止ページはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが使用できないことを通知するには、keepout コマンドを使用します。

例

次に、立ち入り禁止ページを設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSLVPN 接続の属性を設定できます。

kerberos-realm

この Kerberos サーバのレルム名を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **kerberos-realm** コマンドを使用します。レルム名を削除するには、このコマンドの **no** 形式を使用します。

kerberos-realm *string*

no kerberos-realm

構文の説明

string	大文字と小文字が区別される最大 64 文字の英数字ストリング。ストリングにスペースは使用できません。 **（注）** Kerberos 領域名では数字と大文字だけを使用します。セキュリティ アプライアンスでは、*string* 引数に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで追加されました。

使用上のガイドライン

このコマンドは、Kerberos サーバに対してのみ有効です。

Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Windows 2000 Active Directory サーバ上で実行する場合は、*string* 引数の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 引数には、数字と大文字のアルファベットのみを使用する必要があります。**kerberos-realm** コマンドでは、大文字と小文字が区別されます。また、セキュリティ アプライアンスでは、小文字は大文字に変換されません。

例

次のシーケンスは、AAA サーバ ホストの設定に関するコンテキストで Kerberos レルムを「EXAMPLE.COM」に設定するための **kerberos-realm** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション サブモードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

key

AAA サーバに対して NAS を認証するために使用されるサーバ シークレットの値を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **key** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。キーを削除するには、このコマンドの **no** 形式を使用します。

key *key*

no key

構文の説明

key	最大 127 文字の英数字キーワード。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

key の値は、127 文字までの英数字で構成されているキーワードで、TACACS+ サーバ上のキーと同じ値にします。大文字と小文字は区別されます。127 文字を超えて入力された文字があれば無視されます。このキーは、クライアントとサーバの間でやり取りするデータを暗号化するために使用されます。キーは、クライアント システムとサーバ システムの両方で同一である必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。キー（サーバ シークレット）の値は、セキュリティ アプライアンスを AAA サーバに対して認証します。

このコマンドは、RADIUS サーバと TACACS+ サーバに対してのみ有効です。

以前の PIX Firewall のバージョンで使用されていた **aaa-server** コマンドの **key** パラメータは、対応する **key** コマンドに自動的に変換されます。

例

次に、ホスト「1.2.3.4」上で「srvgrp1」という TACACS+ AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、キーを「myexclusivemumblekey」として設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	AAA サーバのコンフィギュレーションを表示します。

keypair

証明する公開キーのキー ペアを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **keypair** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

keypair *name*

no keypair

構文の説明

name	キー ペアの名前を指定します。

デフォルト

デフォルト設定では、キー ペアは含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、central トラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始し、central トラストポイント用に証明するキー ペアを指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
crypto key generate dsa	DSA キーを生成します。
crypto key generate rsa	RSA キーを生成します。
default enrollment	登録パラメータをデフォルト値に戻します。

keysize

ユーザ証明書の登録で、ローカルの Certificate Authority（CA; 認証局）サーバによって生成される公開キーと秘密キーのサイズを指定するには、CA サーバ コンフィギュレーション モードで **keysize** コマンドを使用します。キー サイズをデフォルトの 1024 ビットの長さにリセットするには、このコマンドの **no** 形式を使用します。

keysize {**512** | **768** | **1024** | **2048**}

no keysize

構文の説明

512	証明書の登録で生成される公開キーと秘密キーのサイズを 512 ビットに指定します。
768	証明書の登録で生成される公開キーと秘密キーのサイズを 768 ビットに指定します。
1024	証明書の登録で生成される公開キーと秘密キーのサイズを 1024 ビットに指定します。
2048	証明書の登録で生成される公開キーと秘密キーのサイズを 2048 ビットに指定します。

デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、ローカル CA サーバによってユーザ用に生成される、公開キーと秘密キーのすべてのキー ペアのキーのサイズを 2048 ビットに指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize 2048
hostname(config-ca-server)#
```

次に、ローカル CA サーバによってユーザ用に生成される、公開キーと秘密キーのすべてのキー ペアのキーのサイズを、デフォルトの 1024 ビットの長さにリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no keysize
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

keysize server

ローカルの Certificate Authority（CA; 認証局）サーバによって生成される公開キーと秘密キーのサイズを指定し、CA 独自のキー ペアのサイズを設定するには、CA サーバ コンフィギュレーション モードで **keysize server** コマンドを使用します。キー サイズをデフォルトの 1024 ビットの長さにリセットするには、このコマンドの no 形式を使用します。

keysize server{**512** | **768** | **1024** | **2048**}

no keysize server

構文の説明

512	証明書の登録で生成される公開キーと秘密キーのサイズを 512 ビットに指定します。
768	証明書の登録で生成される公開キーと秘密キーのサイズを 768 ビットに指定します。
1024	証明書の登録で生成される公開キーと秘密キーのサイズを 1024 ビットに指定します。
2048	証明書の登録で生成される公開キーと秘密キーのサイズを 2048 ビットに指定します。

デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、CA 独自の証明書のキー サイズに 2048 ビットを指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize server 2048
hostname(config-ca-server)#
```

次に、CA 独自の証明書のキー サイズを、デフォルトの 1024 ビットの長さにリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no keysize server
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書のキー ペアのサイズを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

kill

Telnet セッションを終了するには、特権 EXEC モードで **kill** コマンドを使用します。

kill *telnet_id*

構文の説明

telnet_id	Telnet セッションの ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

kill コマンドを使用すると、Telnet セッションを終了できます。Telnet セッションの ID を表示するには、**who** コマンドを使用します。Telnet セッションを終了すると、セキュリティ アプライアンスは、警告することなく、すべてのアクティブなコマンドを終了して接続をドロップします。

例

次に、ID「2」の Telnet セッションを終了する例を示します。最初に、アクティブな Telnet セッションのリストを表示するため、**who** コマンドを入力します。次に、ID「2」の Telnet セッションを終了するため、**kill 2** コマンドを入力します。

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

関連コマンド

コマンド	説明
telnet	セキュリティ アプライアンスへの Telnet アクセスを設定します。
who	アクティブな Telnet セッションのリストを表示します。

CHAPTER 18

l2tp tunnel hello コマンド～ log-adj-changes コマンド

l2tp tunnel hello

L2TP over IPSec 接続における hello メッセージ間の間隔を指定するには、グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを使用します。この間隔をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

構文の説明

interval	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。指定できる範囲は 10 ～ 300 秒です。

デフォルト

デフォルトは 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、セキュリティ アプライアンスによる L2TP 接続の物理層に関する問題の検出をイネーブルにします。デフォルトは 60 秒です。60 秒未満の値に設定すると、問題が発生している接続はより早く切断されます。

例

次に、hello メッセージ間の間隔を 30 秒に設定する例を示します。

```
hostname(config)# l2tp tunnel hello 30
```

関連コマンド

コマンド	説明
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	L2TP 接続の詳細を表示します。
vpn-tunnel-protocol l2tp-ipsec	L2TP を特定のトンネル グループのトンネリング プロトコルとしてイネーブルにします。

ldap attribute-map

ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために LDAP 属性マップを作成し、名前を付けるには、グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

構文の説明

map-name	LDAP 属性マップのユーザ定義名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ldap attribute-map コマンドを使用すると、ユーザ独自の属性名と値を Cisco 属性名にマッピングできます。その後、作成された属性マップを LDAP サーバにバインドできます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは、ldap の後にハイフンを入力してください。

（注）　属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、グローバル コンフィギュレーション モードで、情報を入力したり LDAP サーバにバインドする前に myldapmap という名前の LDAP 属性マップを作成するコマンドの例を示します。

```
hostname(config)# ldap attribute-map myldapmap
```

```
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値を Cisco 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-attribute-map（AAA サーバ ホスト モード）

既存のマッピング コンフィギュレーションを LDAP ホストにバインドするには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-attribute-map** コマンドを使用します。バインディングを削除するには、このコマンドの **no** 形式を使用します。

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

構文の説明

map-name	LDAP 属性マッピング コンフィギュレーションを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シスコ定義の LDAP 属性名が使いやすさやその他の要件を満たしていない場合は、独自の属性名を作成し、それをシスコの属性にマッピングして、作成された属性コンフィギュレーションを LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドにより、LDAP 属性マップ モードが開始されます。このコマンドでは、「ldap」の後にハイフンを入力しないでください。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用して、属性マッピング コンフィギュレーションに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバに属性マップ コンフィギュレーションをバインドします。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、myldapmap という名前の既存の属性マップを ldapsvr1 という名前の LDAP サーバにバインドするコマンドの例を示します。

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP 属性マッピング コンフィギュレーションまたはすべての実行属性マッピング コンフィギュレーションを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-base-dn

サーバが認可要求を受信したときに検索を開始する、LDAP 階層内の位置を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭にリセットするには、このコマンドの **no** 形式を使用します。

ldap-base-dn *string*

no ldap-base-dn

構文の説明

string	サーバが認可要求を受信したときに検索を開始する LDAP 階層内の位置を指定する、最大 128 文字のストリング（たとえば、OU=Cisco）。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

リストの先頭から検索を開始します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで変更された既存のコマンドです。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ベース DN を starthere に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP デフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのデフォルト値は、LDAP サーバが必要とする場合にのみ使用されます。LDAP デフォルト値を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]

no ldap-defaults

構文の説明

port	（任意）LDAP サーバ ポートを指定します。このパラメータが指定されていない場合、セキュリティ アプライアンスは標準の LDAP ポート（389）を使用します。
server	LDAP サーバの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバが存在する場合、この値はそのサーバによって上書きされます。

デフォルト

デフォルト設定は設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、デフォルト ポート（389）に LDAP デフォルト値を定義する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-dn

CRL 取得のために認証を要求する LDAP サーバに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバで必要な場合のみ使用されます。LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*

no ldap-dn

構文の説明

password	この認定者名のパスワードを定義します。最大のフィールドの長さは 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。最大のフィールドの長さは 128 文字です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central の X.500 名として CN=admin,OU=devtest,O=engineering、パスワードとして xxzzyy を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
crypto ca trustpoint	CA トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-group-base-dn

ダイナミック アクセス ポリシーによってグループ検索に使用される Active Directory 階層の基本グループを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-group-base-dn** コマンドを使用します。このコマンドを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

構文の説明

string	サーバが検索を開始する Active Directory 階層内の位置を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。たとえば、ou=Employees を指定します。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。グループ検索 DN を指定しない場合、ベース DN から検索が開始されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

ldap-group-base-dn コマンドは、LDAP を使用する Active Directory サーバにのみ適用され、**show ad-groups** コマンドがグループ検索を開始するときに使用する Active Directory 階層レベルを指定します。検索で取得されたグループは、ダイナミック グループ ポリシーによって特定のポリシーの選択基準として使用されます。

例

次に、組織の部門（ou）レベルの Employees から検索を開始するようにグループ ベース DN を設定する例を示します。

```
hostname(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

関連コマンド

コマンド	説明
group-search-timeout	グループのリストについて Active Directory サーバからの応答をセキュリティ アプライアンスが待機する時間を調整します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

ldap-login-dn

システムがバインドするディレクトリ オブジェクトの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-login-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-dn *string*

no ldap-login-dn

構文の説明

string	LDAP 階層内のディレクトリ オブジェクトの名前を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

Microsoft Active Directory サーバなどの一部の LDAP サーバでは、他の LDAP 動作の要求を受け入れる前に、セキュリティ アプライアンスが認証済みバインディングを介してハンドシェイクを確立している必要があります。セキュリティ アプライアンスは、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、セキュリティ アプライアンスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングのディレクトリ オブジェクト名を入力します（たとえば、cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com）。匿名アクセスの場合は、このフィールドをブランクのままにします。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン DN を myobjectname に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-login-password

LDAP サーバのログイン パスワードを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-login-password** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。このパスワードの指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-password *string*

no ldap-login-password

構文の説明

string	最大 64 文字の英数字のパスワード。大文字と小文字は区別されます。パスワードにスペース文字を含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。パスワードの最大長は 64 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン パスワードを obscurepassword に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。

ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-naming-attribute

相対認定者名属性を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-naming-attribute *string*

no ldap-naming-attribute

構文の説明

string	LDAP サーバ上のエントリを一意に識別する、最大 128 文字の英数字の相対認定者名属性を指定します。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LDAP サーバ上のエントリを一意に識別するための、相対認定者名属性を指定します。共通の命名属性は、一般名（cn）とユーザ ID（uid）です。

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 命名属性を cn に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-over-ssl

セキュアな SSL 接続をセキュリティ アプライアンスと LDAP サーバの間で確立するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-over-ssl** コマンドを使用します。接続の SSL をディセーブルにするには、このコマンドの **no** 形式を使用します。

ldap-over-ssl enable

no ldap-over-ssl enable

構文の説明

enable	SSL で LDAP サーバへの接続を保護することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、SSL でセキュリティ アプライアンスと LDAP サーバの間の接続を保護することを指定します。

（注） プレーン テキスト認証を使用している場合は、この機能をイネーブルにすることを推奨します。**sasl-mechanism** コマンドを参照してください。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、セキュリティ アプライアンスと LDAP サーバ ldapsvr1（IP アドレスは 10.10.0.1）の間の接続に対して SSL をイネーブルにするコマンドの例を示します。PLAIN SASL 認証メカニズムも設定します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
sasl-mechanism	LDAP クライアントとサーバの間に SASL 認証を指定します。
server-type	LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

ldap-scope

サーバが認可要求を受信したときに検索する LDAP 階層内の範囲を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-scope *scope*

no ldap-scope

構文の説明

scope	サーバが認可要求を受信したときに検索する LDAP 階層内のレベルの数を指定します。次の値が有効です。 • **onelevel**：ベース DN の 1 つ下のレベルのみを検索します。 • **subtree**：ベース DN の下のレベルをすべて検索します。

デフォルト

デフォルト値は **onelevel** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで変更された既存のコマンドです。

使用上のガイドライン

scope を **onelevel** と指定すると、ベース DN の 1 つ下のレベルのみが検索されるため、検索速度が向上します。**subtree** を指定すると、ベース DN の下のレベルがすべて検索されるため、検索速度が低下します。

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 範囲を subtree に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。

leap-bypass

LEAP バイパスをイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **leap-bypass enable** コマンドを使用します。LEAP バイパスをディセーブルにするには、**leap-bypass disable** コマンドを使用します。実行コンフィギュレーションから LEAP バイパス属性を削除するには、このコマンドの **no** 形式を使用します。このオプションにより、別のグループ ポリシーから LEAP バイパスの値を継承できます。

leap-bypass {**enable | disable**}

no leap-bypass

構文の説明

disable	LEAP バイパスをディセーブルにします。
enable	LEAP バイパスをイネーブルにします。

デフォルト

LEAP バイパスはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LEAP バイパスをイネーブルにすると、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。デバイスは、ユーザ認証ごとに認証を再実行できます。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

（注） 認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティ リスクが発生する可能性があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに LEAP バイパスを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPN ハードウェア クライアントに、トンネルを開始するたびにユーザ名とパスワードによる認証を要求します。
user-authentication	VPN ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

lifetime（CA サーバ モード）

ローカル Certificate Authority（CA; 認証局）証明書、各発行済み証明書、または Certificate Revocation List（CRL; 証明書失効リスト）の有効期間を指定するには、CA サーバ コンフィギュレーション モードで **lifetime** コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

lifetime {ca-certificate | certificate | crl} *time*

no lifetime {**ca-certificate** | **certificate** | **crl**}

構文の説明

ca-certificate	ローカル CA サーバ証明書のライフタイムを指定します。
certificate	CA サーバが発行するすべてのユーザ証明書のライフタイムを指定します。
crl	CRL のライフタイムを指定します。
time	CA 証明書およびすべての発行済み証明書の場合、*time* はその証明書の有効日数を指定します。有効な範囲は、1 ～ 3650 日です。 CRL の場合、*time* は CRL の有効時間数を指定します。CRL の有効な範囲は、1 ～ 720 時間です。

デフォルト

デフォルトのライフタイムは次のとおりです。

- CA 証明書：3 年間
- 発行済み証明書：1 年間
- CRL：6 時間

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

証明書または CRL が有効である日数または時間数を指定すると、このコマンドは、証明書または CRL に含める有効期限を決定します。

例

次に、3 か月間有効な証明書を発行するように CA を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime certificate 90
```

```
hostname(config-ca-server))#
```

次に、2 日間有効な CRL を発行するように CA を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime crl 48
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める証明書失効リストの配布ポイント（CDP）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
show crypto ca server	ローカル CA コンフィギュレーションの詳細を ASCII テキストで表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

limit-resource

マルチ コンテキスト モードでクラスのリソース制限を指定するには、クラス コンフィギュレーション モードで **limit-resource** コマンドを使用します。制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

limit-resource {**all 0** | [**rate**] *resource_name number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

構文の説明

all 0	すべてのリソースの制限を無制限として設定します。
number[**%**]	リソース制限を 1 以上の固定数、またはパーセント記号（%）付きのシステム制限のパーセンテージ（1 ～ 100）として指定します。無制限のリソースを指定するには、制限を **0** に設定します。システム制限がないリソースの場合は、パーセンテージ（%）を設定できません。絶対値のみを設定できます。
rate	リソースの 1 秒あたりのレートを設定することを指定します。1 秒あたりのレートを設定できるリソースについては、表 18-1 を参照してください。
resource_name	制限を設定するリソース名を指定します。この制限は、**all** に設定されている制限を上書きします。

デフォルト

すべてのリソースは無制限に設定されています。ただし、デフォルトでコンテキストごとに許可される最大値に設定される次の制限を除きます。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

クラスのリソースを制限した場合、セキュリティ アプライアンスは、クラスに割り当てられた各コンテキストのためにリソースの一部を確保するのではなく、セキュリティ アプライアンスはコンテキストに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。

表 18-1 に、リソース タイプと制限を示します。**show resource types** コマンドも参照してください。

（注） 「システム制限」カラムに「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。

表 18-1　リソース名と制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
conns	同時またはレート	該当なし	同時接続数：プラットフォームの接続制限については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。
inspects	レート	該当なし	該当なし	アプリケーション インスペクション。
hosts	同時接続数	該当なし	該当なし	セキュリティ アプライアンス経由で接続可能なホスト。
asdm	同時接続数	最小 1 最大 5	32	ASDM 管理セッション。 **（注）** ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション
syslogs	レート	該当なし	該当なし	システム ログ メッセージ。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
member	コンテキストをリソース クラスに割り当てます。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

lmfactor

最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再検証ポリシーを設定するには、キャッシュ コンフィギュレーション モードで **lmfactor** コマンドを使用します。このようなオブジェクトを再検証するための新しいポリシーを設定するには、このコマンドを再度使用します。属性をデフォルト値 20 にリセットするには、このコマンドの **no** 形式を使用します。

lmfactor *value*

no lmfactor

構文の説明

value	0 ～ 100 の範囲の整数。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、lmfactor の値を使用して、キャッシュされたオブジェクトを変更なしと見なす時間の長さを推定します。これは有効期限と呼ばれます。セキュリティ アプライアンスは、最終変更後の経過時間に lmfactor をかけることによって有効期限を推定します。

lmfactor を 0 に設定すると、ただちに再検証が強制されます。100 に設定すると、再検証までの時間は可能な限り長くなります。

例

次に、lmfactor を 30 に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。

コマンド	説明
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **log** コマンドを使用して、**match** コマンドまたはクラス マップに一致するパケットをログに記録します。このログ アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で使用できます。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

log

no log

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照する）、**log** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットをログに記録できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットが http-traffic クラス マップに一致する場合にログを送信する例を示します。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

log-adj-changes

OSPF ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

構文の説明

detail	（任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

log-adj-changes コマンドはデフォルトでイネーブルになっています。このコマンドの **no** 形式で削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPF ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

CHAPTER 19

logging asdm コマンド～ logout message コマンド

logging asdm

システム ログ メッセージを ASDM ログ バッファに送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	ASDM ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

ASDM のロギングはデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

ASDM のログ バッファが満杯の場合、セキュリティ アプライアンス はメッセージを古いものから削除して、新しいメッセージのためのバッファ スペースを確保します。ASDM ログ バッファに保持されるシステム ログ メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM ログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは異なります。

例

ロギングをイネーブルにして、重大度レベル 0、1、2 のメッセージを ASDM ログ バッファに送信する例を示します。また、ASDM ログ バッファ サイズを 200 メッセージに設定する例も示します。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファに含まれているすべてのメッセージをクリアします。
logging asdm-buffer-size	ASDM ログ バッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	ロギング設定を表示します。

logging asdm-buffer-size

ASDM ログ バッファに保持されるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログ バッファをデフォルトのサイズの 100 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

構文の説明

num_of_msgs	ASDM ログ バッファでセキュリティ アプライアンスが保持するシステム ログ メッセージの数を指定します。

デフォルト

デフォルトの ASDM syslog バッファ サイズは 100 メッセージです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のログ バッファが満杯の場合、セキュリティ アプライアンス はメッセージを古いものから削除して、新しいメッセージのためのバッファ スペースを確保します。ASDM ログ バッファへのロギングをイネーブルにするかどうかを制御するには、または ASDM ログ バッファに保持されるシステム ログ メッセージの種類を制御するには、**logging asdm** コマンドを使用します。

ASDM ログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは異なります。

例

ロギングをイネーブルにして、重大度レベル 0、1、2 のメッセージを ASDM ログ バッファに送信する例を示します。また、ASDM ログ バッファ サイズを 200 メッセージに設定する例も示します。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
```

```
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファに含まれているすべてのメッセージをクリアします。
logging asdm	ASDM ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging buffered

セキュリティ アプライアンスによってシステム ログ メッセージをログ バッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファ サイズは 4 KB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、セキュリティ アプライアンスはバッファを消去してから、メッセージの追加を続行します。ログ バッファがいっぱいになると、セキュリティ アプライアンスでは最も古いメッセージを削除して、バッファに新しいメッセージ用の領域を確保します。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** コマンドおよび **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信するシステム ログ メッセージは、**show logging** コマンドで確認できます。

例

次に、レベル 0 および 1 のイベントに対してバッファへのロギングを設定する例を示します。

```
hostname(config)# logging buffered alerts
hostname(config)#
```

次の例では、最大ロギング レベル 7 の notif-list というリストを作成し、notif-list リストで識別されるシステム ログ メッセージに対して、バッファへのロギングを設定します。

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging buffer-size

ログ バッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログ バッファをデフォルトのサイズの 4 KB のメモリにリセットするには、このコマンドの **no** 形式を使用します。

logging buffer-size *bytes*

no logging buffer-size *bytes*

構文の説明

bytes	ログ バッファに使用するメモリ量をバイト単位で設定します。たとえば、8192 を指定した場合、セキュリティ アプライアンスによってログ バッファに 8 KB のメモリが使用されます。

デフォルト

ログ バッファ サイズは 4 KB メモリです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのバッファ サイズと異なるサイズのログ バッファがセキュリティ アプライアンスによって使用されているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合は、セキュリティ アプライアンスによって 4 KB のログ バッファが使用されています。

セキュリティ アプライアンスによるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ロギング バッファをイネーブルにして、セキュリティ アプライアンスがログ バッファに 16 KB のメモリを使用することを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging class

メッセージ クラスに対して、ロギング先ごとの最大ロギング レベルを設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージ クラスのロギング レベル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

logging class *class destination level* [*destination level* . . .]

no logging class *class*

構文の説明

class	ロギング先ごとの最大ロギング レベルのメッセージ クラスを指定します。class の有効な値については、後述する「使用上のガイドライン」を参照してください。
destination	*class* に対してロギング先を指定します。ロギング先について、*destination* に送信される最大ロギング レベルは *level* によって決まります。*destination* の有効な値については、後述する「使用上のガイドライン」を参照してください。
level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL

デフォルト

デフォルトでは、セキュリティ アプライアンス はロギング先およびメッセージ クラス単位ではロギング レベルを適用しません。ロギング先をイネーブルに設定したときに指定したロギング リストまたはレベルに基づいて決定されたロギング レベルで、イネーブルの各ロギング先が全クラスのメッセージを受け取ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	有効な class の値に **eigrp** が追加されました。

使用上のガイドライン

class の有効な値は次のとおりです。

- **auth**：ユーザ認証
- **bridge**：トランスペアレント ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **eap**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **eigrp**：EIGRP ルーティング
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **nac**：ネットワーク アドミッション コントロール 初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント

- **vpnfo**：VPN フェールオーバー
- **vpnlb**：VPN ロード バランシング

有効なロギング先は、次のとおりです。

- **asdm**：このロギング先については、**logging asdm** コマンドを参照してください。
- **buffered**：このロギング先については、**logging buffered** コマンドを参照してください。
- **console**：このロギング先については、**logging console** コマンドを参照してください。
- **history**：このロギング先については、**logging history** コマンドを参照してください。
- **mail**：このロギング先については、**logging mail** コマンドを参照してください。
- **monitor**：このロギング先については、**logging monitor** コマンドを参照してください。
- **trap**：このロギング先については、**logging trap** コマンドを参照してください。

例

次に、フェールオーバー関連メッセージについて、ASDM ログ バッファの最大ロギング レベルが 2、システム ログ バッファの最大ロギング レベルが 7 であることを指定する例を示します。

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging console

セキュリティ アプライアンスでシステム ログ メッセージをコンソール セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。コンソール セッションへのシステム ログ メッセージの表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]

no logging console

（注） バッファ オーバーフローが原因で多数のシステム ログ メッセージがドロップされる可能性があるため、このコマンドは使用しないことを推奨します。詳細については、後述する「使用上のガイドライン」を参照してください。

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスでシステム ログ メッセージはコンソール セッションに表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンソールにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

注意　**logging console** コマンドを使用すると、システム パフォーマンスが大幅に低下する可能性があります。代わりに、**logging buffered** コマンドを使用してロギングを開始し、**show logging** コマンドを使用してメッセージを表示します。最新のメッセージをより簡単に表示するには、**clear logging buffer** コマンドを使用してバッファをクリアします。

例

次に、ロギング レベル 0、1、2、および 3 のシステム ログ メッセージをコンソール セッションに表示できるようにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging debug-trace

デバッグ メッセージを重大度レベル 7 で発行されるシステム ログ メッセージ 711001 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。デバッグ メッセージのログへの送信を停止するには、このコマンドの **no** 形式を使用します。

logging debug-trace

no logging debug-trace

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはデバッグ出力をシステム ログ メッセージに含めません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ メッセージは重大度レベル 7 のメッセージとして生成されます。システム ログ メッセージ番号 711001 でログに表示されますが、モニタリング セッションには表示されません。

例

次に、ロギングをイネーブルに設定し、システム ログ バッファにログ メッセージを送信し、ログにデバッグ出力を転送し、ディスク動作のデバッグをオンにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

ログに示されるデバッグ メッセージの例は、次のとおりです。

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging device-id

EMBLEM 形式でないシステム ログ メッセージにデバイス ID を含めるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **logging device-id** コマンドを使用します。デバイス ID の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

構文の説明

context-name	現在のコンテキストの名前をデバイス ID として指定します。
hostname	セキュリティ アプライアンスのホスト名をデバイス ID として指定します。
ipaddress *interface_name*	デバイス ID または *interface_name* のインターフェイスの IP アドレスを指定します。**ipaddress** キーワードを使用すると、外部サーバに送信されるシステム ログ メッセージには、外部サーバへのログ データの送信にセキュリティ アプライアンスで使用されるインターフェイスに関係なく、指定したインターフェイスの IP アドレスが含まれます。
string *text*	最大 16 文字の *text* で指定された文字をデバイス ID として指定します。スペースおよび次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：未満 • >：より大きい • ?：疑問符

デフォルト

システム ログ メッセージにデフォルトのデバイス ID は使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ipaddress キーワードを使用すると、メッセージが送信されるインターフェイスに関係なく、デバイス ID は指定したセキュリティ アプライアンス インターフェイスの IP アドレスとなります。このキーワードにより、そのデバイスから送信されるすべてのメッセージに対して、単一の一貫したデバイス ID が指定されます。

例

次の例は、secappl-1 というホストを設定する方法を示しています。

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

ホスト名は、次のメッセージなどのシステム ログ メッセージの先頭に表示されます。

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging emblem

syslog サーバ以外のロギング先に送信されるシステム ログ メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging emblem

no logging emblem

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスでシステム ログ メッセージに EMBLEM 形式は使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバ以外のすべてのロギング先に対して、EMBLEM 形式のロギングをイネーブルにすることができます。**logging timestamp** キーワードもイネーブルにする場合、タイム スタンプが付与されたメッセージが送信されます。

syslog サーバに対して EMBLEM 形式のロギングをイネーブルにするには、**logging host** コマンドで **format emblem** オプションを使用します。

例

次に、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して EMBLEM 形式の使用をイネーブルにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging enable

設定済みの出力場所すべてに対してロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging enable

no logging enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ロギングはデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先へのシステム ログ メッセージの送信をイネーブルまたはディセーブルにすることができます。**no logging enable** コマンドを使用して、すべてのロギングを停止できます。

次のコマンドを使用して、個別のロギング先へのロギングをイネーブルにすることができます。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次に、ロギングをイネーブルにする例を示します。**show logging** コマンドの出力は、使用可能な各ロギング先を個別にイネーブルにする必要がある状況を示しています。

```
hostname(config)# logging enable
```

```
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging facility

syslog サーバに送信されるメッセージに使用するロギング ファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギング ファシリティをデフォルトの 20 にリセットするには、このコマンドの **no** 形式を使用します。

logging facility *facility*

no logging facility

構文の説明

facility	ロギング ファシリティを指定します。有効な値は、16 ～ 23 です。

デフォルト

デフォルトのファシリティは 20（LOCAL4）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。例外については、「構文の説明」を参照してください。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

syslog サーバでは、メッセージはメッセージの *facility* 番号に基づいてファイルされます。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

この例では、セキュリティ アプライアンスでシステム ログ メッセージのロギング ファシリティを 16 に指定する例を示します。**show logging** コマンドの出力には、セキュリティ アプライアンスによって使用されているファシリティが含まれます。

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
```

```
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging flash-bufferwrap

未保存のメッセージでログ バッファがいっぱいになるたびに、セキュリティ アプライアンスでバッファをフラッシュ メモリに書き込めるようにするには、グローバル コンフィギュレーション モードで **logging flash-bufferwrap** コマンドを使用します。フラッシュ メモリへのログ バッファの書き込みをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging flash-bufferwrap

no logging flash-bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスによってログ バッファがフラッシュ メモリに書き込まれるようにするには、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに書き込まれません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスはフラッシュ メモリにログ バッファの内容を書き込んでいる間も、新しいイベント メッセージをログ バッファに格納し続けます。

セキュリティ アプライアンスは、次のようなデフォルトのタイムスタンプ形式を使用した名前のログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

logging flash-bufferwrap コマンドを使用する場合、フラッシュ メモリの可用性が、セキュリティ アプライアンスによるシステム ログ メッセージの保存方法に影響します。詳細については、**logging flash-maximum-allocation** コマンドおよび **logging flash-minimum-free** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
copy	TFTP サーバまたは FTP サーバを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-maximum-allocation	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するために、セキュリティ アプライアンスで使用可能にする必要があるフラッシュ メモリの最小量を指定します。
show logging	イネーブルなロギング オプションを表示します。

logging flash-maximum-allocation

ログ データを保管するためにセキュリティ アプライアンスで使用するフラッシュ メモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。この目的に使用するフラッシュ メモリの最大量をデフォルト サイズの 1 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

構文の説明

kbytes	ログ バッファ データを保存するためにセキュリティ アプライアンスで使用できるフラッシュ メモリの最大量（KB 単位）。

デフォルト

ログ データ用のデフォルトの最大フラッシュ メモリ割り当ては 1 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュ メモリの量が決まります。

logging savelog または **logging flash-bufferwrap** で保存されるログ ファイルにより、ログ ファイル用のフラッシュ メモリの使用が **logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、セキュリティ アプライアンスによって最も古いログ ファイルが削除され、新しいログ ファイル用に十分なメモリが解放されます。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリが新しいログ ファイルには小さすぎる場合は、セキュリティ アプライアンスで新しいログ ファイルを保存できません。

デフォルトのサイズとは異なるサイズの最大フラッシュ メモリ割り当てがセキュリティ アプライアンスにあるかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、セキュリティ アプライアンスでは保存されるログ バッファ データに対して最大 1 MB が使用されています。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

セキュリティ アプライアンスによるログ バッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにし、ログ ファイルの書き込みに使用されるフラッシュ メモリの最大量を約 1.2 MB に設定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するために、セキュリティ アプライアンスで使用可能にする必要があるフラッシュ メモリの最小量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging flash-minimum-free

セキュリティ アプライアンスで新しいログ ファイルを保存する前に存在している必要があるフラッシュ メモリの最小空き領域を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。このコマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドによって作成されたログ ファイルをセキュリティ アプライアンスで保存する前に存在している必要があるフラッシュ メモリの空き領域に影響します。フラッシュ メモリの必要最小空き領域をデフォルト サイズの 3 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

構文の説明

kbytes	セキュリティ アプライアンスで新しいログ ファイルを保存する前に使用可能にしておく必要のあるフラッシュ メモリの最小量（KB 単位）。

デフォルト

フラッシュ メモリのデフォルトの最小の空き容量は 3 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

logging flash-minimum-free コマンドでは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に保持しておく必要があるフラッシュ メモリの量を指定します。

logging savelog または **logging flash-bufferwrap** で保存されるログ ファイルにより、フラッシュ メモリの空き領域が **logging flash-minimum-free** コマンドで指定された制限を下回る場合、セキュリティ アプライアンスによって最も古いログ ファイルが削除され、新しいログ ファイルの保存後も最小量のメモリが空きのまま残るようにします。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリがまだ制限を下回る場合、セキュリティ アプライアンスで新しいログ ファイルを保存できません。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにし、フラッシュ メモリの最小空き領域が 4000 KB である必要があることを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging from-address

セキュリティ アプライアンスによって送信されるシステム ログ メッセージの送信元電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging from-address** コマンドを使用します。送信されるすべてのシステム ログ メッセージは、指定したアドレスから送信されたように表示されます。送信元電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。

logging from-address *from-email-address*

no logging from-address *from-email-address*

構文の説明

from-email-address	送信元電子メール アドレス。つまり、システム ログ メッセージの送信元として表示される電子メール アドレス（cdb@example.com など）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

電子メールによるシステム ログ メッセージの送信は、**logging mail** コマンドでイネーブルにします。

このコマンドで指定するアドレスは、既存の電子メール アカウントに対応している必要はありません。

例

ロギングをイネーブルにし、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定するには、次の基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
```

```
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	セキュリティ アプライアンスの電子メールによるシステム ログ メッセージの送信をイネーブルにし、電子メールで送信するメッセージを決定します。
logging recipient-address	システム ログ メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging ftp-bufferwrap

未保存のメッセージでログ バッファがいっぱいになるたびに、セキュリティ アプライアンスが FTP サーバにログ バッファを送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。FTP サーバへのログ バッファの送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging ftp-bufferwrap

no logging ftp-bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバへのログ バッファの送信はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

logging ftp-bufferwrap をイネーブルにすると、セキュリティ アプライアンスにより、ログ バッファ データは **logging ftp-server** コマンドで指定した FTP サーバに送信されます。セキュリティ アプライアンスは FTP サーバにログ データを送信しているいる間も、新しいイベント メッセージをログ バッファに格納し続けます。

セキュリティ アプライアンスによってログ バッファの内容が FTP サーバに送信されるようにするには、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに書き込まれません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、次のようなデフォルトのタイムスタンプ形式を使用した名前のログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにして、FTP サーバを指定し、セキュリティ アプライアンスが FTP サーバにログ バッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs でアクセスできます。ログ ファイルは、/syslogs ディレクトリに格納されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバ パラメータを指定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging ftp-server

logging ftp-bufferwrap がイネーブルの場合にセキュリティ アプライアンスによってログ バッファ データが送信される FTP サーバの詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバの詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

構文の説明

0	（任意）暗号化されていない（クリア テキストの）ユーザ パスワードが続くことを指定します。
8	（任意）暗号化されたユーザ パスワードが続くことを指定します。
ftp-server	外部 FTP サーバの IP アドレスまたはホスト名。 **（注）** ホスト名を指定する場合は、ネットワーク上で DNS が正しく動作していることを確認してください。
password	指定したユーザ名のパスワード。
path	ログ バッファ データが保存される FTP サーバ上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次に例を示します。 `/security_appliances/syslogs/appliance107`
username	FTP サーバへのログインに有効なユーザ名。

デフォルト

デフォルトでは、FTP サーバは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(5)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

FTP サーバは 1 つのみ指定できます。ロギング FTP サーバがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、その FTP サーバ コンフィギュレーションが、入力した新しいコンフィギュレーションに置き換えられます。

セキュリティ アプライアンス は、指定された FTP サーバ情報を確認しません。詳細を誤って設定した場合、セキュリティ アプライアンスによってログ バッファ データを FTP サーバに送信できません。

セキュリティ アプライアンスの起動時またはアップグレード時に、1 桁のパスワードや、1 桁の数値で始まりその後に空白が指定されたパスワードはサポートされません。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにして、FTP サーバを指定し、セキュリティ アプライアンスが FTP サーバにログ バッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs でアクセスできます。ログ ファイルは、/syslogs ディレクトリに格納されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
```

次に、暗号化されたパスワードを入力する例を示します。

```
hostname(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

次に、暗号化されていない（クリア テキストの）パスワードを入力する例を示します。

```
hostname(config)# logging ftp-server logserver /path1 user1 0 pass1
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging history

SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging history [*logging_list* | *level*]

no logging history

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	SNMP サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスによって SNMP サーバにロギングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバへのロギングをイネーブルにし、SNMP メッセージ レベルまたはイベント リストを設定できます。

例

次に、SNMP ロギングをイネーブルにし、ロギング レベル 0、1、2、および 3 のメッセージが設定した SNMP サーバに送信されることを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
snmp-server	SNMP サーバの詳細を指定します。

logging host

syslog サーバを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバ定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**] [**permit-hostdown**]

logging host *interface_name syslog_ip*

[**no**] **logging host** *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

[**no**] **logging host** *interface_name syslog_ip*

構文の説明

format emblem	（任意）syslog サーバに対して EMBLEM 形式のロギングをイネーブルにします。
interface_name	syslog サーバが配置されているインターフェイスを指定します。
permit-hostdown	syslog サーバがダウンしているか、または到達不能である場合に、適応型セキュリティ アプライアンスが TCP ロギングを続行できるようにします。
port	syslog サーバがメッセージをリッスンするポートを指定します。有効なポート値は、いずれのプロトコルの場合も 1025 ～ 65535 です。
secure	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 **（注）** セキュアなロギング接続は、SSL/TLS 対応の syslog サーバとのみ確立できます。SSL/TLS 接続を確立できない場合、新しい接続はすべて拒否されます。このデフォルトの動作は、**logging permit-hostdown** コマンドを入力して変更できます。
syslog_ip	syslog サーバの IP アドレスを指定します。
tcp	セキュリティ アプライアンスによって syslog サーバへのメッセージの送信に TCP が使用されることを指定します。
udp	セキュリティ アプライアンスによって syslog サーバへのメッセージの送信に UDP が使用されることを指定します。

デフォルト

デフォルト プロトコルは UDP です。

デフォルトのポート番号は次のとおりです。

- UDP：514
- TCP：1470

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(2)	**secure** キーワードが追加されました。

使用上のガイドライン

logging host *ip_address* **format emblem** コマンドを使用すると、各 syslog サーバに対して EMBLEM 形式のロギングをイネーブルにすることができます。EMBLEM 形式のロギングは、UDP システム ログ メッセージのみに使用できます。EMBLEM 形式のロギングを特定の syslog サーバに対してイネーブルにすると、メッセージはそのサーバに送信されます。**logging timestamp** キーワードもイネーブルにする場合、タイム スタンプが付与されたメッセージが送信されます。

複数の **logging host** コマンドを使用して、追加サーバを指定できます。それらすべてでシステム ログ メッセージが受信されます。ただし、UDP と TCP 両方ではなく、いずれかのシステム ログ メッセージのみが受信されるようにサーバを指定できます。

（注）　**logging host** コマンドで **tcp** オプションを使用すると、syslog サーバに到達できない場合、ファイアウォールを通過する接続は適応型セキュリティ アプライアンスによってドロップされます。

以前入力した *port* と *protocol* の値だけを表示するには、**show running-config logging** コマンドを使用して、リストからコマンドを見つけます（TCP は 6、UDP は 17 として表示されます）。TCP ポートは syslog サーバのみで機能します。*port* は、syslog サーバがリッスンするポートと同じである必要があります。

（注）　**logging host** コマンドと **secure** キーワードを UDP で使用しようとすると、エラー メッセージが表示されます。

PIX セキュリティ アプライアンスは **secure** キーワードをサポートしません。

例

次の例は、デフォルトのプロトコルとポート番号を使用する内部インターフェイス上の syslog サーバに、重大度 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging list

さまざまな基準（ログ レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために、他のコマンドで使用するロギング リストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

構文の説明

class *event_class*	（任意）システム ログ メッセージのイベントのクラスを設定します。指定したレベルについて、指定したクラスのシステム ログ メッセージのみがコマンドによって識別されます。クラスのリストについては、「使用上のガイドライン」を参照してください。
level *level*	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
message *start_id*[**-***end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルト レベルを検索するには、**show logging** コマンドを使用するか、または『*Cisco ASA 5500 Series System Log Messages*』を参照してください。
name	ロギング リスト名を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class で使用できる値は、次のとおりです。

- **auth**：ユーザ認証
- **bridge**：トランスペアレント ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **eap**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **nac**：ネットワーク アドミッション コントロール 初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント
- **vpnfo**：VPN フェールオーバー

- **vpnlb**：VPN ロード バランシング

例

次に、logging list コマンドの使用例を示します。

```
hostname(config)# logging list my-list message 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

上の例では、指定した基準に一致するシステム ログ メッセージがロギング バッファに送信されるように指定しています。この例で指定されている基準は、次のとおりです。

- 100100 ～ 100110 の範囲内のシステム ログ メッセージ ID
- 重大度が critical 以上（emergency、alert、または critical）のすべてのシステム ログ メッセージ
- warning レベル以上（emergency、alert、critical、error、または warning）にある VPN クラスのすべてのシステム ログ メッセージ

システム ログ メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注） リストの条件を設定するときには、条件が重なり合うメッセージ セットを指定できます。複数の基準と一致するシステム ログ メッセージも正常にロギングされます。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging mail

セキュリティ アプライアンスでシステム ログ メッセージを電子メールで送信できるようにし、電子メールで送信するメッセージを判別できるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。システム ログ メッセージの電子メール送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

電子メールへのロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

電子メールで送信されるシステム ログ メッセージは、送信された電子メールの件名欄に表示されます。

例

電子メールでシステム ログ メッセージを送信するようにセキュリティ アプライアンスを設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示される電子メール アドレスを指定します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging message

システム ログ メッセージのログ レベルを指定するには、グローバル コンフィギュレーション モードで **logging message** コマンドを **level** キーワードとともに使用します。メッセージのログ レベルをデフォルトのレベルにリセットするには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスで特定のシステム ログ メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（**level** キーワードは指定しません）。セキュリティ アプライアンスで特定のシステム ログ メッセージを生成できるようにするには、**logging message** コマンドを使用します（**level** キーワードは指定しません）。これら 2 つのバージョンの **logging message** コマンドは、並行して使用できます。後述する「例」を参照してください。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

構文の説明

level *level*	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
syslog_id	イネーブルまたはディセーブルにするシステム ログ メッセージまたは重大度レベルを変更する syslog メッセージの ID。メッセージのデフォルト レベルを検索するには、**show logging** コマンドを使用するか、または『*Cisco ASA 5500 Series System Log Messages*』を参照してください。

デフォルト

デフォルトでは、すべてのシステム ログ メッセージはイネーブルであり、すべてのメッセージの重大度レベルはデフォルトのレベルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging message コマンドは、次の 2 つの目的で使用できます。

- メッセージをイネーブルにするかディセーブルにするかを制御します。
- メッセージの重大度レベルを制御します。

show logging コマンドを使用して、メッセージに現在割り当てられている重大度レベルや、メッセージがイネーブルかどうかを判別できます。

例

次に、**logging message** コマンドの一連の使用例を示します。これらの例では、メッセージをイネーブルにするかどうか、およびメッセージの重大度レベルの両方を制御しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	すべてのロギング コンフィギュレーションまたはメッセージ コンフィギュレーションのみをクリアします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging monitor

セキュリティ アプライアンスでシステム ログ メッセージを SSH セッションおよび Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。SSH セッションおよび Telnet セッションへのシステム ログ メッセージの表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]

no logging monitor

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	SSH セッションまたは Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスによってシステム ログ メッセージは SSH セッションおよび Telnet セッションに表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging monitor コマンドにより、現在のコンテキストのすべてのセッションに対してシステム ログ メッセージがイネーブルになります。ただし、各セッションでは **terminal** コマンドによって、システム ログ メッセージがそのセッションに表示されるかどうかが制御されます。

例

次に、コンソール セッションでシステム ログ メッセージの表示をイネーブルにする例を示します。**errors** キーワードの使用は、ロギング レベル 0、1、2、および 3 のメッセージが SSH セッションおよび Telnet セッションに表示されることを示しています。**terminal** コマンドを使用すると、現在のセッションでメッセージを表示できます。

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCP ベースの syslog サーバのステータスを新しいユーザ セッションと無関係にするには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバが使用できないときにセキュリティ アプライアンスで新しいユーザ セッションを拒否するには、このコマンドの **no** 形式を使用します。

logging permit-hostdown

no logging permit-hostdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、TCP 接続を使用する syslog サーバへのロギングをイネーブルにした場合、何らかの理由で syslog サーバが使用できないときに、セキュリティ アプライアンスでは新しいネットワーク アクセス セッションを許可しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

syslog サーバへメッセージを送信するためのロギング トランスポート プロトコルとして TCP を使用している場合、セキュリティ アプライアンスが syslog サーバに到達できないときに、セキュリティ アプライアンスではセキュリティ対策として新しいネットワーク アクセス セッションを拒否します。**logging permit-hostdown** コマンドを使用して、この制限を削除できます。

例

次に、TCP ベースの syslog サーバのステータスを、セキュリティ アプライアンスで新しいセッションが許可されるかどうかと無関係にする例を示します。**logging permit-hostdown** コマンドの出力に **show running-config logging** コマンドが含まれている場合、TCP ベースの syslog サーバのステータスは、新しいネットワーク アクセス セッションと無関係です。

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging queue

ロギング コンフィギュレーションに従って処理する前にセキュリティ アプライアンスのキューに保持できるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギング キューのサイズをデフォルトの 512 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging queue *queue_size*

no logging queue *queue_size*

構文の説明

queue_size	処理前の syslog メッセージを保管するために使用されるキューで許可される syslog メッセージの数。有効な値は、プラットフォームの種類に応じて 0 ～ 8192 メッセージです。ロギング キューが 0 に設定されている場合、プラットフォームに応じて、キューは設定可能な最大サイズ（8192 メッセージ）になります。ASA-5505 では、最大キュー サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

デフォルト

デフォルトのキュー サイズは 512 メッセージです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

トラフィックが多いためにキューがいっぱいになった場合、セキュリティ アプライアンスによってメッセージが廃棄される場合があります。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

例

次に、**logging queue** コマンドおよび **show logging queue** コマンドの出力を表示する例を示します。

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、**logging queue** コマンドは 0 に設定されています。つまり、キューは最大の 8192 に設定されます。キュー内のシステム ログ メッセージは、セキュリティ アプライアンスによって、ロギング コンフィギュレーションで指定された方法で処理されます。たとえば、システム ログ メッセージをメールの受信者に送信したり、フラッシュ メモリに保存したりします。

この例の **show logging queue** コマンドの出力には、5 つのメッセージがキューにあり、セキュリティ アプライアンスが最後に起動されてから同時にキューにあった最大メッセージ数は 3513 メッセージであり、1 つのメッセージが廃棄されたことが示されています。キューは無制限として設定されていますが、キューにメッセージを追加するためのブロック メモリがなかったため、メッセージが廃棄されました。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging rate-limit

システム ログ メッセージの生成レートを制限するには、特権 EXEC モードで **logging rate-limit** コマンドを使用します。レート制限をディセーブルにするには、特権 EXEC モードでこのコマンドの **no** 形式を使用します。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

構文の説明

interval	（任意）メッセージの生成レートを測定するために使用する時間間隔（秒単位）。*interval* 値の有効な範囲は、0 ～ 2147483647 です。
level *severity_level*	設定されたレート制限を、特定の重大度レベルに属するすべてのシステム ログ メッセージに適用します。指定した重大度レベルのすべてのシステム ログ メッセージは、個別にレート制限されます。*severity_level* の有効な範囲は、1 ～ 7 です。
message	このシステム ログ メッセージのレポートを抑制します。
num	指定した時間間隔中に生成できるシステム メッセージ数。*num* 値の有効な範囲は、0 ～ 2147483647 です。
syslog_id	抑制されるシステム ログ メッセージの ID。有効な値の範囲は 100000 ～ 999999 です。
unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。

デフォルト

interval のデフォルト設定は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

システム メッセージの重大度は次のとおりです。

- 0：システム使用不可
- 1：ただちに対応
- 2：重大な状況
- 3：エラー メッセージ

•4：警告メッセージ

•5：通知だけ、重要な状況ではない

•6：Informational（情報）

•7：デバッグ メッセージ

例

システム ログ メッセージの生成レートを制限するには、特定のメッセージ ID を入力します。次に、特定のメッセージ ID と時間間隔を使用してシステム ログ メッセージの生成レートを制限する例を示します。

```
hostname(config)# logging rate-limit 100 600 message 302020
```

この例では、指定した 600 秒の間隔でレート制限 100 に達すると、システム ログ メッセージ 302020 はホストに送信されなくなります。

システム ログ メッセージの生成レートを制限するには、特定の重大度レベルを入力します。次に、特定の重大度レベルと時間間隔を使用してシステム ログ メッセージの生成レートを制限する例を示します。

```
hostname(config)# logging rate-limit 1000 600 level 6
```

この例では、重大度レベル 6 未満のすべてのシステム ログ メッセージが、指定した 600 秒の時間間隔で指定したレート制限 1000 に抑制されます。重大度 6 のシステム ログ メッセージのレート制限はそれぞれ 1000 です。

関連コマンド

コマンド	説明
clear running-config logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	現在内部バッファ内にあるメッセージを表示するか、ロギング コンフィギュレーションの設定を表示します。
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

セキュリティ アプライアンスによって送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。最大 5 つの受信者アドレスを設定できます。必要に応じて、受信者アドレスごとに、**logging mail** コマンドで指定されたメッセージ レベルとは異なるメッセージ レベルを指定できます。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

構文の説明

address	システム ログ メッセージを電子メールで送信する際の受信者の電子メール アドレスを指定します。
level	ロギング レベルがこの後に続くことを示します。
level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL **（注）** **logging recipient-address** コマンドで 3 より大きいレベルを使用することは推奨できません。ロギング レベルを大きくすると、バッファ オーバーフローによってシステム ログ メッセージがドロップされる可能性があります。 **logging recipient-address** コマンドで指定されたメッセージ レベルは、**logging mail** コマンドで指定されたメッセージ レベルを上書きします。たとえば、**logging recipient-address** コマンドでロギング レベル 7 を指定すると、**logging mail** コマンドでレベル 3 を指定していても、セキュリティ アプライアンスはロギング レベル 4、5、6、および 7 を含め、すべてのメッセージを受信側に送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

電子メールによるシステム ログ メッセージの送信は、**logging mail** コマンドでイネーブルにします。

最大 5 つの **logging recipient-address** コマンドを設定できます。コマンドごとに異なるロギング レベルを指定できます。このコマンドは、緊急性の高いメッセージを緊急性の低いメッセージよりも多くの受信者に送信する場合に便利です。

例

電子メールでシステム ログ メッセージを送信するようにセキュリティ アプライアンスを設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	システム ログ メッセージの送信元として表示される電子メール アドレスを指定します。
logging mail	セキュリティ アプライアンスの電子メールによるシステム ログ メッセージの送信をイネーブルにし、電子メールで送信するメッセージを決定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging savelog

ログ バッファをフラッシュ メモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

構文の説明

savefile	（任意）保存するフラッシュ メモリ ファイルの名前。ファイル名を指定しない場合は、次に示すように、ログ ファイルはセキュリティ アプライアンスによってデフォルトのタイムスタンプ フォーマットを使用して保存されます。 LOG-*YYYY-MM-DD-HHMMSS*.TXT *YYYY* は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

デフォルト

デフォルトの設定は次のとおりです。

- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。
- デフォルトのログ ファイル名については、「構文の説明」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存する前に、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保存されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

（注）　**logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

例

次に、ロギングとログ バッファを有効にし、グローバル コンフィギュレーション モードを終了して、フラッシュ メモリへファイル名 latest-logfile.txt を使用してログ バッファを保存する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
copy	TFTP サーバまたは FTP サーバを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

logging standby

フェールオーバー スタンバイセキュリティ アプライアンスでこのセキュリティ アプライアンスのシステム ログ メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。システム ログのメッセージングおよび SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging standby

no logging standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

logging standby コマンドは、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging standby をイネーブルにして、フェールオーバーの発生時にフェールオーバー スタンバイセキュリティ アプライアンスのシステム ログ メッセージを同期されたままにすることができます。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、FTP サーバなどの共有ロギング先でのトラフィックは 2 倍になります。

例

次に、セキュリティ アプライアンスでシステム ログ メッセージをフェールオーバー スタンバイ セキュリティ アプライアンスに送信できるようにする例を示します。**show logging** コマンドの出力から、この機能がイネーブルであることがわかります。

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
```

```
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
failover	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging timestamp

メッセージが生成された日付と時刻をシステム ログ メッセージに含めることを指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。日付と時刻をシステム ログ メッセージから削除するには、このコマンドの **no** 形式を使用します。

logging timestamp

no logging timestamp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

セキュリティ アプライアンスでは、デフォルトでは日付と時刻はシステム ログ メッセージに含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging timestamp コマンドを使用すると、セキュリティ アプライアンスによってすべてのシステム ログ メッセージにタイムスタンプが含まれます。

例

次に、すべてのシステム ログ メッセージにタイムスタンプ情報が含まれるようにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging trap

セキュリティ アプライアンスによって syslog サーバに送信されるシステム ログ メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。コンフィギュレーションからこのコマンドを削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]

no logging trap

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	syslog サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトのシステム ログ メッセージのトラップは定義されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ロギング トランスポート プロトコルとして TCP を使用している場合、セキュリティ アプライアンスが syslog サーバに到達できないか、syslog サーバが誤って設定されているか、ディスクがいっぱいになると、セキュリティ アプライアンスではセキュリティ対策として新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングでは、syslog サーバに障害が発生しても、セキュリティ アプライアンスによるトラフィックの送信は停止されません。

例

次の例は、内部インターフェイス上に存在し、デフォルトのプロトコルとポート番号を使用する syslog サーバに、ロギング レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

login

ローカル ユーザ データベースを使用して特権 EXEC モードにログインするか（username コマンドを参照）、ユーザ名を変更するには、ユーザ EXEC モードで **login** コマンドを使用します。

login

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ユーザ EXEC モードから、**login** コマンドを使用して、ローカル データベース内の任意のユーザ名として特権 EXEC モードにログインできます。認証をオンにした場合、**login** コマンドは **enable** コマンドと類似しています（**aaa authentication console** コマンドを参照）。enable 認証と異なり、**login** コマンドではローカル ユーザ名データベースのみを使用でき、認証が常に必要です。CLI モードから **login** コマンドを使用して、ユーザを変更することもできます。

ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization コマンド**を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用できます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

例

次に、**login** コマンドを入力した後のプロンプトの例を示します。

```
hostname> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのためのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンド アクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザをローカル データベースに追加します。

login-button

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのログイン ボタンをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン ボタン テキストは「Login」です。

デフォルトのログイン ボタン スタイルは、次のとおりです。

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログイン ボタンをテキスト「OK」でカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

関連コマンド

コマンド	説明
login-title	WebVPN ページ ログイン ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

login-message

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-message** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン メッセージは、「Please enter your username and password」です。

デフォルトのログイン メッセージのスタイルは、background-color:#CCCCCC;color:black です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次の例では、ログイン メッセージのテキストは「username and password」に設定されます。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
username-prompt	WebVPN ページ ログインのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページ ログインのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページ ログインのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザに表示される WebVPN ページのログイン ボックスのタイトルをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-title** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン テキストは「Login」です。

ログイン タイトルのデフォルトの HTML スタイルは、background-color: #666666; color: white です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログイン タイトルのスタイルを設定する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

関連コマンド

コマンド	説明
login-message	WebVPN ログイン ページのログイン メッセージをカスタマイズします。
username-prompt	WebVPN ログイン ページのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ログイン ページのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ログイン ページのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのロゴをカスタマイズするには、webvpn カスタマイゼーション モードで **logo** コマンドを使用します。コンフィギュレーションからロゴを削除してデフォルト（Cisco ロゴ）にリセットするには、このコマンドの **no** 形式を使用します。

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

構文の説明

file	ロゴを含むファイルを指定することを示します。
none	ロゴがないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。
path	ファイル名のパス。可能なパスは、disk0:、disk1:、または flash: です。
value	ロゴのファイル名を指定します。最大長は 255 文字です（スペースを含めることはできません）。ファイル タイプは JPG、PNG、または GIF であり、100 KB 未満である必要があります。

デフォルト

デフォルトのロゴは Cisco ロゴです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

指定したファイル名が存在しない場合は、エラー メッセージが表示されます。ロゴ ファイルを削除したが、コンフィギュレーションがまだそのファイルを指している場合、ロゴは表示されません。

ファイル名にスペースを含めることはできません。

例

次の例では、ファイル cisco_logo.gif にカスタム ロゴが含まれています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

関連コマンド

コマンド	説明
title	WebVPN ページのタイトルをカスタマイズします。
page style	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータを使用して WebVPN ページをカスタマイズします。

logout

CLI を終了するには、ユーザ EXEC モードで **logout** コマンドを使用します。

logout

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logout コマンドを使用すると、セキュリティ アプライアンスからログアウトできます。**exit** コマンドまたは **quit** コマンドを使用して、ユーザ モードに戻ることができます。

例

次に、セキュリティ アプライアンスからログアウトする例を示します。

```
hostname> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

WebVPN ユーザが WebVPN サービスからログアウトするときに表示される WebVPN ログアウト画面のログアウト メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **logout-message** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログアウト メッセージ テキストは「Goodbye」です。

デフォルトのログアウト メッセージのスタイルは、background-color:#999999;color:black です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログアウト メッセージのスタイルを設定する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
italic; font-weight: bold
```

関連コマンド

コマンド	説明
logout-title	WebVPN ページのログアウト タイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

CHAPTER 20

mac address コマンド～ multicast-routing コマンド

mac address

アクティブ ユニットおよびスタンバイ ユニットの仮想 MAC アドレスを指定するには、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

構文の説明

phy_if	MAC アドレスを設定するインターフェイスの物理名です。
active_mac	アクティブ ユニットの仮想 MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。
standby_mac	スタンバイ ユニットの仮想 MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。

デフォルト

デフォルトの設定は次のとおりです。

- アクティブ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*02

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

仮想 MAC アドレスがフェールオーバー グループに対して定義されていない場合は、デフォルト値が使用されます。

同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover mac address	物理インターフェイスの仮想 MAC アドレスを指定します。

mac-address

プライベート MAC アドレスをインターフェイスまたはサブインターフェイスに手動で割り当てるには、インターフェイス コンフィギュレーション モードで **mac-address** コマンドを使用します。マルチコンテキスト モードでは、このコマンドは各コンテキストでそれぞれ別の MAC アドレスをインターフェイスに割り当てることができます。MAC アドレスをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

mac-address *mac_address* [**standby** *mac_address*]

no mac-address [*mac_address* [**standby** *mac_address*]]

構文の説明

mac_address	このインターフェイスの MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。フェールオーバーを使用する場合は、この MAC アドレスがアクティブな MAC アドレスとなります。 **（注）** 自動生成されたアドレス（**mac-address auto** コマンド）は A2 で始まるため、A2 を含む手動 MAC アドレスは自動生成を使用しようとしても開始できません。
standby *mac_address*	（任意）フェールオーバーのスタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

デフォルト

デフォルトの MAC アドレスは、物理インターフェイスのバーンドイン MAC アドレスです。サブインターフェイスは、物理インターフェイスの MAC アドレスを継承します。一部のコマンド（シングル モードでのこのコマンドを含む）は物理インターフェイスの MAC アドレスを設定するため、継承されるアドレスはその設定によって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(5)	**mac-address auto** コマンドと併用するときには、MAC アドレスを開始する A2 の使用が制限されました。

使用上のガイドライン

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有した場合、各コンテキストでそれぞれ固有の MAC アドレスをインターフェイスに割り当てることができます。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

このコマンドで各 MAC アドレスを手動で割り当てることができます。あるいは **mac-address auto** コマンドを使用して、コンテキストで共有インターフェイスの MAC アドレスを自動的に生成できます。MAC アドレスを自動的に生成する場合、**mac-address** コマンドを使用して、生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

他のコマンドまたは方式で MAC アドレスを設定することもできます。MAC アドレスの設定方法には次の優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスとサブインターフェイスに対して使用します。マルチ コンテキスト モードでは、MAC アドレスを各コンテキスト内で設定します。この機能を使用すると、複数のコンテキストの同じインターフェイスに異なる MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードでの Active/Standby フェールオーバーのための **failover mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードでの Active/Active フェールオーバーのための **mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードでの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキストの共有インターフェイスに適用されます。

5. Active/Active フェールオーバーの場合の物理インターフェイスのためのアクティブ MAC アドレスおよびスタンバイ MAC アドレスの自動生成。

   この方法は、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は、物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

例

次に、GigabitEthernet 0/1.1 の MAC アドレスを設定する例を示します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address auto	マルチ コンテキスト モードでの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address auto

プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てるには、グローバル コンフィギュレーション モードで **mac-address auto** コマンドを使用します。自動 MAC アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address auto prefix *prefix*

no mac-address auto

構文の説明

prefix *prefix*	MAC アドレスの一部として使用されるプレフィックスを設定します。*prefix* は、0 ～ 65535 の 10 進数です。このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各セキュリティ アプライアンスはそれぞれ固有の MAC アドレスを使用するようになるため、次のように 1 つのネットワーク セグメントに複数のセキュリティ アプライアンスを配置できます。プレフィックスの使用方法の詳細については、「MAC Address Format」を参照してください。

デフォルト

自動生成はデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(5)	**prefix** キーワードが追加されました。プレフィックスを使用し、固定の開始値（A2）を使用し、フェールオーバー ペアのプライマリ ユニットおよびセカンダリ ユニットの MAC アドレスで別の方式を使用するように、MAC アドレス形式が変更されました。MAC アドレスは現在、リロード間で持続されるようになっています。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。

使用上のガイドライン

インターフェイスを共有するコンテキストを許可するには、固有の MAC アドレスを各共有コンテキスト インターフェイスに割り当てることを推奨します。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先ア

ドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MAC アドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MAC アドレスを手動で設定するには、**mac-address** コマンドを参照してください。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

自動生成された MAC アドレスはすべて、A2 で始まります。自動生成された MAC アドレスは、リロード間で持続されます。

手動 MAC アドレスとの通信

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。

自動生成されたアドレスは A2 で始まるため、手動 MAC アドレスを A2 で始めることはできません。たとえ自動生成も使用する予定であってもそれは同じです。

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、セキュリティ アプライアンスはインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。詳細については、「MAC Address Format」を参照してください。

prefix キーワードが導入される前に従来のバージョンの **mac-address auto** コマンドを使用してフェールオーバー ユニットをアップグレードする場合は、「prefix キーワードを使用しない従来の MAC アドレス形式」の項を参照してください。

MAC Address Format

セキュリティ アプライアンスは、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザ定義のプレフィックスで、zz.zzzz はセキュリティ アプライアンスが生成した内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、セキュリティ アプライアンスは 77 を 16 進数値 004D（yyxx）に変換します。MAC アドレスで使用すると、プレフィックスはセキュリティ アプライアンスネイティブ形式に一致するように逆にされます（xxyy）。

A24**D.00**zz.zzzz

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03**zz.zzzz

MAC アドレスが生成される場合

コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規 MAC アドレスが生成されます。コンテキスト インターフェイスを設定した後でこのコマンドをイネーブルにした場合、コマンドを入力するとただちにすべてのインターフェイスの MAC アドレスが生成されます。**no**

mac-address auto コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

他の方法を使用した MAC アドレスの設定

他のコマンドまたは方式で MAC アドレスを設定することもできます。MAC アドレスの設定方法には次の優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスとサブインターフェイスに対して使用します。マルチ コンテキスト モードでは、MAC アドレスを各コンテキスト内で設定します。この機能を使用すると、複数のコンテキストの同じインターフェイスに異なる MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードでの Active/Standby フェールオーバーのための **failover mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードでの Active/Active フェールオーバーのための **mac address** コマンド。

   このコマンドは、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードでの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキストの共有インターフェイスに適用されます。

5. Active/Active フェールオーバーの場合の物理インターフェイスのためのアクティブ MAC アドレスおよびスタンバイ MAC アドレスの自動生成。

   この方法は、物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は、物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** または **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

システム コンフィギュレーションでの MAC アドレスの表示

システム実行スペースから割り当てられた MAC アドレスを表示するには、**show running-config all context** コマンドを入力します。

割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。このコマンドはグローバル コンフィギュレーション モードでのみユーザによる設定が可能ですが、**mac-address auto** コマンドは割り当てられた MAC アドレスとともに各コンテキストのコンフィギュレーションに読み取り専用エントリとして表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

（注） MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

コンテキスト内の MAC アドレスの表示

コンテキスト内の各インターフェイスで使用されている MAC アドレスを表示するには、**show interface | include (Interface)|(MAC)** コマンドを入力します。

（注）　**show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

prefix キーワードを使用しない従来の MAC アドレス形式

バージョン 8.0(5) 以前、**mac-address auto** コマンドには **prefix** キーワードが含まれていませんでした。この旧バージョンのコマンドは引き続き使用できるため、フェールオーバー ペア間でアップグレードを実行できます。アップグレードしても自動的に変換されないため、このコマンドはアップグレードしたフェールオーバー ユニットとアップグレードしなかったフェールオーバー ユニット間でこれまでどおり一致したものとなります。両ユニットを新しいソフトウェア バージョンにアップグレードした後には、**prefix** キーワードを使用するようにこのコマンドを変更する必要があります。

prefix キーワードがないと、MAC アドレスは次の形式で生成されます。

- アクティブ ユニットの MAC アドレス：12*_slot.port_subid.contextid*.
- スタンバイ ユニットの MAC アドレス：02*_slot.port_subid.contextid*.

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* は、**show context detail** コマンドで表示可能なコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

この従来の MAC アドレス生成方法では、リロード間で MAC アドレスが持続されず、同じネットワーク セグメントに複数のセキュリティ アプライアンスを配置できず（固有の MAC アドレスが保証されないため）、手動で割り当てた MAC アドレスとの MAC アドレスの重複が回避されません。

例

次に、プレフィックス 78 で自動 MAC アドレス生成をイネーブルにする例を示します。

```
hostname(config)# mac-address auto prefix 78
```

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
hostname# show running-config all context
```

```
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブとスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address-table aging-time

MAC アドレス テーブルのエントリにタイムアウトを設定するには、グローバル コンフィギュレーション モードで **mac-address-table aging-time** コマンドを使用します。デフォルト値の 5 分に戻すには、このコマンドの **no** 形式を使用します。

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

構文の説明

timeout_value	タイムアウトするまで MAC アドレス エントリが MAC アドレス テーブルにとどまることができる時間。有効な値は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

デフォルト

デフォルトのタイムアウトは 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

使用方法のガイドラインはありません。

例

次に、MAC アドレスのタイムアウトを 10 分に設定する例を示します。

```
hostname(config)# mac-address-timeout aging time 10
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

mac-address-table static

MAC アドレス テーブルにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。MAC アドレスは通常、特定の MAC アドレスからのトラフィックがインターフェイスに入るときに MAC アドレス テーブルにダイナミックに追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

構文の説明

interface_name	送信元インターフェイス。
mac_address	テーブルに追加する MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、スタティック MAC アドレスのエントリを MAC アドレス テーブルに追加する例を示します。

```
hostname(config)# mac-address-table static inside 0010.7cbe.6101
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。

コマンド	説明
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

mac-learn

インターフェイスの MAC アドレス ラーニングをディセーブルにするには、グローバル コンフィギュレーション モードで **mac-learn** コマンドを使用します。MAC アドレス ラーニングを再びイネーブルにするには、このコマンドの **no** 形式を使用します。デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、セキュリティ アプライアンスは対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできます。

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

構文の説明

interface_name	MAC アドレス学習をディセーブルにするインターフェイス。
disable	MAC 学習をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、外部インターフェイスでの MAC アドレス学習をディセーブルにする例を示します。

```
hostname(config)# mac-learn outside disable
```

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** コンフィギュレーションをデフォルトに設定します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。

コマンド	説明
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。
show running-config mac-learn	**mac-learn** コンフィギュレーションを表示します。

mac-list

認証や許可から MAC アドレスを削除するのに使用される MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC アドレス リストのエントリを削除するには、このコマンドの **no** 形式を使用します。

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

構文の説明

deny	この MAC アドレスに一致するトラフィックは MAC アドレス リストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方の対象となることを示します。ffff.ffff.0000 などの MAC アドレス マスクを使用して、ある範囲の MAC アドレスを許可し、その範囲の MAC アドレスを強制的に認証および許可する場合には、MAC アドレス リストに拒否エントリを追加することが必要になる場合があります。
id	MAC アクセス リストの 16 進数値を指定します。一連の MAC アドレスをグループ化するには、同じ ID 値で必要な回数の **mac-list** コマンドを入力します。パケットが最適に一致するエントリではなく最初に一致するエントリを使用するため、エントリの順序が重要になります。permit エントリがあり、その permit エントリで許可されているアドレスを拒否する場合は、permit エントリよりも前に deny エントリを入力してください。
mac	送信元 MAC アドレスを 12 桁の 16 進数形式、つまり、nnnn.nnnn.nnnn で指定します。
macmask	MAC アドレスのどの部分を照合に使用するかを指定します。たとえば、ffff.ffff.ffff は完全に MAC アドレスと一致します。ffff.ffff.0000 は最初の 8 桁だけ一致します。
permit	この MAC アドレスに一致するトラフィックは MAC アドレス リストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方から削除されることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

認証および許可からの MAC アドレスの削除をイネーブルにするには、**aaa mac-exempt** コマンドを使用します。1 つの **aaa mac-exempt** コマンドのみを追加できるため、削除するすべての MAC アドレスが MAC アドレス リストに含まれていることを確認してください。複数の MAC リストを作成できますが、一度に使用できるのは 1 つだけです。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次の例では、00a0.c95d.02b2 以外の MAC アドレス グループの認証をバイパスします。00a0.c95d.02b2 は permit ステートメントとも一致するため、permit ステートメントよりも前に deny ステートメントを入力します。permit ステートメントが前にある場合、deny ステートメントとは一致しません。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
clear configure mac-list	**mac-list** コマンドで指定されている MAC アドレスのリストを削除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。

mail-relay

ローカル ドメイン名を設定するには、パラメータ コンフィギュレーション モードで **mail-relay** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

構文の説明

domain_name	ドメイン名を指定します。
drop-connection	接続を閉じます。
log	システム ログ メッセージを生成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、特定のドメインへのメール中継を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mail-relay mail action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

management-access

VPN の使用時にセキュリティ アプライアンスへの通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスを許可するには、グローバル コンフィギュレーション モードで **management-access** コマンドを使用します。管理アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

management-access *mgmt_if*

no management-access *mgmt_if*

構文の説明

mgmt_if	別のインターフェイスからセキュリティ アプライアンスに入るときにアクセスする管理インターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドを使用すると、フル トンネル IPSec VPN または SSL VPN クライアント（AnyConnect 2.x クライアント、SVC 1.x）を使用するときや、サイトツーサイト IPSec トンネルを横断するときには、セキュリティ アプライアンスへの通過ルートとなるインターフェイス以外のインターフェイスに接続できます。たとえば、外部インターフェイスからセキュリティ アプライアンスに入る場合、このコマンドを使用すると、Telnet で内部インターフェイスに接続できます。あるいは、外部インターフェイスから入るときには、内部インターフェイスに ping を実行できます。

次のアプリケーションを使用できます。

- SNMP ポーリング
- HTTPS 要求
- ASDM アクセス
- Telnet アクセス
- SSH アクセス
- ping
- Syslog ポーリング

- NTP 要求

管理アクセス インターフェイスは 1 つだけ定義できます。

（注）　管理アクセス インターフェイスにスタティック NAT ステートメントは適用されません。適用した場合、リモート VPN ユーザが管理インターフェイスにアクセスできなくなります。

例

次に、ファイアウォール インターフェイスを管理アクセス インターフェイスとして「inside」という名前で設定する例を示します。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
show management-access	管理アクセスのために設定された内部インターフェイスの名前を表示します。

management-only

管理トラフィックのみを受け付けるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **management-only** コマンドを使用します。通過トラフィックを許可するには、このコマンドの **no** 形式を使用します。

management-only

no management-only

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA 5510 以降の適応型セキュリティ アプライアンス上の Management 0/0 インターフェイスは、デフォルトでは管理専用モードに設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 という専用の管理インターフェイスが含まれ、セキュリティ アプライアンスへのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の場合、管理専用モードをディセーブルにできるため、このインターフェイスは他のインターフェイスと同じくトラフィックを通過させることができます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。セキュリティ アプライアンスまたはコンテキストには割り当てられ、個々のインターフェイスには割り当てられない管理 IP アドレスとは別のサブネットにこのインターフェイスを配置する場合、トランスペアレント モードでこのインターフェイスの IP アドレスを設定することもできます。

例

次に、管理インターフェイスで管理専用モードをディセーブルにする例を示します。

```
hostname(config)# interface management0/0
hostname(config-if)# no management-only
```

次に、サブインターフェイスで管理専用モードをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# management-only
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

map-name

ユーザ定義の属性名をシスコ属性名にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドを使用します。

このマッピングを削除するには、このコマンドの **no** 形式を使用します。

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

構文の説明

user-attribute-name	シスコ属性にマッピングするユーザ定義の属性名を指定します。
Cisco-attribute-name	ユーザ定義の属性名にマッピングするシスコ属性名を指定します。

デフォルト

デフォルトでは、名前のマッピングはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-name コマンドでは、ユーザ定義の属性名をシスコ属性名にマッピングできます。その後、作成された属性マップを LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは「ldap」の後にハイフンを付けます。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ myldapmap でユーザ定義の属性名 Hours をシスコ属性名 cVPN3000-Access-Hours にマッピングする例を示します。

```
hostname(config)# ldap attribute-map myldapmap
```

```
hostname(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
hostname(config-ldap-attribute-map)#
```

LDAP 属性マップ モードでは、次の例に示すように、「?」を入力してシスコ LDAP 属性名の詳細なリストを表示できます。

```
hostname(config-ldap-attribute-map)# map-name ?
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

map-value

ユーザ定義の値をシスコ LDAP 属性にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-value** コマンドを使用します。マップ内のエントリを削除するには、このコマンドの **no** 形式を使用します。

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

構文の説明

cisco-value-string	シスコ属性のシスコ値ストリングを指定します。
user-attribute-name	シスコ属性名にマッピングするユーザ定義の属性名を指定します。
user-value-string	シスコ属性値にマッピングするユーザ定義の値のストリングを指定します。

デフォルト

デフォルトでは、シスコ属性にマッピングされるユーザ定義の値がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-value コマンドでは、ユーザ定義の属性値をシスコ属性名および属性値にマッピングできます。作成された属性マップは、LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは「ldap」の後にハイフンを付けます。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ モードを開始し、ユーザ定義の属性 Hours のユーザ定義の値をユーザ定義の時間ポリシー workDay とシスコ定義の時間ポリシー Daytime に設定する例を示します。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-value Hours workDay Daytime
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP マップを削除します。

mask

モジュラ ポリシー フレームワークを使用する場合、一致コンフィギュレーション モードまたはクラス コンフィギュレーション モードで **mask** コマンドを使用して、**match** コマンドと一致するパケットの一部またはクラス マップをマスクして除外します。この mask アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。たとえば、セキュリティ アプライアンスでのトラフィックの通過を許可する前に、DNS アプリケーション インスペクションに **mask** コマンドを使用してヘッダー フラグをマスクします。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

mask [**log**]

no mask [**log**]

構文の説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力して、アプリケーション トラフィック（**class** コマンドは、**match** コマンドが含まれている既存の **class-map type inspect** コマンドを参照します）を識別した後、**mask** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するパケットの一部をマスクできます。

レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。ここで dns_policy_map はインスペクション ポリシー マップの名前です。

例

次に、セキュリティ アプライアンスでのトラフィックの通過を許可する前に、DNS ヘッダーで RD フラグおよび RA フラグをマスクする例を示します。

```
hostname(config-cmap)# policy-map type inspect dns dns-map1
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log
hostname(config-pmap-c)# match header-flag RA
hostname(config-pmap-c)# mask log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

mask-banner

サーバ バナーを難読化するには、パラメータ コンフィギュレーション モードで **mask-banner** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mask-banner

no mask-banner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、サーバ バナーをマスクする例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

mask-syst-reply

FTP サーバ応答をクライアントから見えないようにするには、**ftp-map** コマンドを使用してアクセスできる FTP マップ コンフィギュレーション モードで **mask-syst-reply** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

mask-syst-reply

no mask-syst-reply

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
FTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

クライアントから FTP サーバ システムを保護するには、厳格な FTP インスペクションで mask-syst-reply コマンドを使用します。このコマンドをイネーブルにすると、**syst** コマンドに対するサーバからの応答は一連の X に置き換えられます。

例

次に、セキュリティ アプライアンスで syst コマンドに対する FTP サーバの応答を一連の X に置き換える例を示します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-map)#
```

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。

match access-list

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match access-list** コマンドを使用して、アクセス リストに基づいてアクションを適用するトラフィックを特定します。**match access-list** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match access-list *access_list_name*

no match access-list *access_list_name*

構文の説明

access_list_name	一致条件として使用するアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションを適用するレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**match access-list** コマンドを入力してトラフィックを識別できます。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。クラス マップには 1 つの **match access-list** コマンドのみを含めることができ、他のタイプの **match** コマンドとは組み合わせることができません。セキュリティ アプライアンスでインスペクトできるすべてのアプリケーションが使用するデフォルトの TCP ポートおよび UDP ポートを照合する **match default-inspection-traffic** コマンドを定義する場合は、例外として **match access-list** コマンドを使用して照合するトラフィックの範囲を絞り込めます。**match default-inspection-traffic** コマンドによって照合するポートが指定されるため、アクセス リストのポートはすべて無視されます。

2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。

3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。

4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、3 つのアクセス リストに一致する 3 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match any

モジュラ ポリシー フレームワーク を使用するときは、クラス マップ コンフィギュレーション モードで **match any** コマンドを使用して、アクションを適用するすべてのトラフィックを一致させます。**match any** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match any

no match any

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションを適用するレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**match any** コマンドを入力してすべてのトラフィックを識別できます。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。**match any** コマンドは、他のタイプの **match** コマンドとは組み合わせることができません。

2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、クラス マップおよび **match any** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match any
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従ってトラフィックを照合します。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match apn

GTP メッセージのアクセス ポイント名に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match apn** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、GTP インスペクション クラス マップのアクセス ポイント名に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match apn class gtp_regex_apn
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match body

ESMTP 本文メッセージの長さまたは 1 行の長さに対して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match body** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **body [length | line length] gt** *bytes*

no match [**not**] **body [length | line length] gt** *bytes*

構文の説明

length	ESMTP 本文メッセージの長さを指定します。
line length	ESMTP 本文メッセージの 1 行の長さを指定します。
bytes	一致する数値をバイト単位で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップで本文 1 行の長さに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match body line length gt 1000
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match called-party

H.323 着信側に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match called-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **called-party** [**regex** *regex*]

no match [**not**] **match** [**not**] **called-party** [**regex** *regex*]

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション クラス マップで着信側に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match called-party regex caller1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match calling-party

H.323 発信側に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match calling-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **calling-party** [**regex** *regex*]

no match [**not**] **match** [**not**] **calling-party** [**regex** *regex*]

構文の説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション クラス マップで発信側に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match calling-party regex caller1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match certificate

PKI 証明書検証プロセス中、セキュリティ アプライアンスは証明書失効ステータスを確認してセキュリティを確保します。また、CRL チェックまたは Online Certificate Status Protocol（OCSP）を使用してこのタスクを完了できます。CRL チェックでは、セキュリティ アプライアンスは失効した証明書の詳細なリストである証明書失効リストを取得、解析、およびキャッシュします。OCSP は失効ステータスを確認する拡張性の高い方法であり、検証局で証明書ステータスをローカライズします。この検証局が特定の証明書のステータスを問い合わせます。

証明書一致ルールには、OCSP URL オーバーライドを設定できます。このオーバーライドには、リモート ユーザ証明書の AIA フィールドの URL ではなく、失効ステータスを確認するための URL を指定します。一致ルールには、OCSP 応答側証明書の検証に使用するトラストポイントも設定できます。これにより、セキュリティ アプライアンスは自己署名証明書やクライアント証明書の検証パスの外部にある証明書など任意の CA からの応答側証明書を検証できます。

証明書一致ルールを設定するには、クリプト CA トラストポイント モードで **match certificate** コマンドを使用します。コンフィギュレーションからルールを削除するには、このコマンドの **no** 形式を使用します。

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

構文の説明

map-name	このルールに一致する証明書マップの名前を指定します。一致ルールを設定する前に、証明書マップを設定する必要があります。最大 65 文字です。
match certificate	この一致ルールの証明書マップを指定します。
override ocsp	ルールの目的が証明書の OCSP URL を上書きすることであることを指定します。
seq-num	この一致ルールのプライオリティを設定します。指定できる範囲は、1 ～ 10000 です。セキュリティ アプライアンスは、まずシーケンス番号が最も小さな一致ルールを評価し、それから順に一致が見つかるまで高い番号の一致ルールを評価していきます。
trustpoint	（任意）トラストポイントを使用して OCSP 応答側証明書を確認することを指定します。
trustpoint-name	（任意）応答側証明書を検証するために オーバーライドとともに使用するトラストポイントを特定します。
url	OCSP 失効ステータスの URL にアクセスすることを指定します。
URL	OCSP 失効ステータスのためにアクセスする URL を識別します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　OCSP を設定するときは、次のヒントに留意してください。

- 1 つのトラストポイント コンフィギュレーション内に複数の一致ルールを設定できますが、各クリプト CA 証明書マップに指定できる一致ルールは 1 つだけです。ただし、複数のクリプト CA 証明書マップを設定し、それらを同じトラストポイントに関連付けることができます。
- 一致ルールを設定する前に、証明書マップを設定する必要があります。
- 自己署名 OCSP 応答側証明書を検証するようにトラストポイントを設定するには、自己署名応答側証明書を信頼できる CA 証明書として独自のトラストポイントにインポートします。次に、自己署名 OCSP 応答側証明書が含まれているトラストポイントを使用して応答側証明書を検証するように、トラストポイントを検証するクライアント証明書の **match certificate** コマンドを設定します。同じことが、クライアント証明書の検証パスの外部にある応答側証明書の検証にも当てはまります。
- クライアント証明書と応答側証明書の両方を同じ CA が発行している場合には、1 つのトラストポイントでどちらも検証できます。しかし、クライアント証明書と応答側証明書を発行している CA が異なる場合は、トラストポイントを証明書ごとに 1 つずつ計 2 つ設定する必要があります。
- OCSP サーバ（応答側）証明書は一般に、OCSP 応答に署名します。セキュリティ アプライアンスが応答を受け取ると、応答側の証明書を検証しようとします。CA は通常、自身の OCSP 応答側証明書のライフタイムを比較的短い期間に設定して、証明書が侵害される可能性を最小限に抑えます。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータス チェックが必要ないことを示します。しかし、この拡張が含まれていない場合、セキュリティ アプライアンスはトラストポイントに指定されているものと同じ方法で自身の失効ステータスをチェックしようとします。応答側証明書が検証可能でない場合、失効チェックは失敗します。このような失敗を回避するには、トラストポイントを検証する応答側証明書には **revocation-check none** を設定し、クライアント証明書には **revocation-check ocsp** を設定します。
- セキュリティ アプライアンスは、一致が見つからない場合、**ocsp url** コマンドの URL を使用します。**ocsp url** コマンドを設定しなかった場合は、リモート ユーザ証明書の AIA フィールドが使用されます。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例　次に、newtrust という名前のトラストポイントの証明書一致ルールを作成する例を示します。ルールには、マップ名 mymap、シーケンス番号 4、トラストポイント mytrust があり、URL として 10.22.184.22 が指定されています。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

```
hostname(config-ca-trustpoint)#
```

その次に、クリプト CA 証明書マップを段階的に設定し、CA 証明書が含まれているトラストポイントを識別して応答側証明書を検証するための一致証明書ルールを設定する例を示します。これが必要になるのは、newtrust トラストポイントで識別した CA が OCSP 応答側証明書を発行していない場合です。

ステップ 1　マップ ルールの適用先のクライアント証明書を識別する証明書マップを設定します。この例では、証明書マップの名前は mymap で、シーケンス番号は 1 です。サブジェクト名に mycert という CN 属性が含まれているクライアント証明書はどれも、mymap エントリに一致します。

```
hostname(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
hostname(config-ca-cert-map)#
```

ステップ 2　OCSP 応答側証明書の検証に使用する CA 証明書が含まれているトラストポイントを設定します。自己署名証明書の場合、これは自己署名証明書自体であり、インポートされてローカルに信頼できるようになっています。この目的で外部の CA 登録を介して証明書を取得することもできます。CA 証明書に貼り付けるように求められたら貼り付けます。

```
hostname(config-ca-cert-map)# exit
hostname(config)# crypto ca trustpoint mytrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

ステップ 3　OCSP を失効チェック方法にして、元のトラストポイント newtrust を設定します。次に、ステップ 2 で設定した証明書マップ mymap および自己署名トラストポイント mytrust を含めた一致ルールを設定します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

クライアント証明書認証に newtrust トラストポイントを使用する接続はどれも、mymap 証明書マップに指定されている属性ルールにクライアント証明書が一致するかどうかを確認します。一致する場合、セキュリティ アプライアンスは 10.22.184.22 にある OCSP 応答側にアクセスして証明書失効ステータスを確認します。次に、mytrust トラストポイントを使用して、応答側証明書を検証します。

（注） newtrust トラストポイントは、OCSP 経由でクライアント証明書の失効チェックを実行するように設定されます。ただし、mytrust トラストポイントにはデフォルトの失効チェック方法が設定されています。デフォルトは none であるため、OCSP 応答側証明書に対して失効チェックは実行されません。

関連コマンド

コマンド	説明
crypto ca certificate map	クリプト CA 証明書マップを作成します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

match cmd

ESMTP コマンド verb に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match cmd** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

no match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

構文の説明

verb *verb*	ESMTP コマンド verb を指定します。
line length gt *bytes*	1 行の長さを指定します。
RCPT count gt *recipients_number*	受信者の電子メール アドレスの数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP トランザクションで交換される verb（メソッド）NOOP に関して一致条件を ESMTP インスペクション ポリシー マップに設定する例を示します。

```
hostname(config-pmap)# match cmd verb NOOP
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match default-inspection-traffic

クラス マップに inspect コマンドのデフォルトのトラフィックを指定するには、クラス マップ コンフィギュレーション モードで **match default-inspection-traffic** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match default-inspection-traffic

no match default-inspection-traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

各インスペクションのデフォルトのトラフィックについては、「使用上のガイドライン」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match default-inspection-traffic コマンドを使用すると、個々の **inspect** コマンドのデフォルトのトラフィックを照合できます。**match default-inspection-traffic** コマンドは、一般に **permit ip** *src-ip dst-ip* という形式のアクセス リストであるもう 1 つの match コマンドと併用できます。

match default-inspection-traffic コマンドともう 1 つの match コマンドを組み合わせるためのルールは、**match default-inspection-traffic** コマンドを使用してプロトコルおよびポート情報を指定し、別の **match** コマンドを使用して他のすべての情報（IP アドレスなど）を指定するというものです。もう 1 つの **match** コマンドに指定されているプロトコルやポート情報は、**inspect** コマンドでは無視されます。

たとえば、次の例に指定されているポート 65535 は無視されます。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# match port 65535
```

インスペクション用のデフォルトのトラフィックは、次のようになります。

インスペクション タイプ	プロトコル タイプ	送信元ポート	宛先ポート
ctiqbe	tcp	該当なし	1748
dcerpc	tcp	該当なし	135
dns	udp	53	53
ftp	tcp	該当なし	21
gtp	udp	2123、3386	2123、3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718 ～ 1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
im	tcp	該当なし	1 ～ 65539
ipsec-pass-thru	udp	該当なし	500
mgcp	udp	2427、2727	2427、2727
netbios	udp	137 ～ 138	該当なし
rpc	udp	111	111
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sip	tcp,udp	該当なし	5060
skinny	tcp	該当なし	2000
smtp	tcp	該当なし	25
sqlnet	tcp	該当なし	1521
tftp	udp	該当なし	69
xdmcp	udp	177	177

例

次に、クラス マップおよび **match default-inspection-traffic** コマンドを使用してトラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-class

DNS Resource Record or Question セクションの Domain System Class に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match dns-class** コマンドを使用します。設定済みのクラスを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

構文の説明

eq	完全一致を指定します。
c_well_known	既知の名前 IN で DNS クラスを指定します。
c_val	DNS クラス フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
c_val1 c_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージのすべてのフィールド（質問および RR）を調べ、指定されたクラスを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS クラスに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-class eq IN
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-type

クエリー タイプや RR タイプなど DNS タイプに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match dns-type** コマンドを使用します。設定された DNS タイプを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

構文の説明

eq	完全一致を指定します。
t_well_known	A、NS、CNAME、SOA、TSIG、IXFR、AXFR のいずれかの既知の名前で DNS タイプを指定します。
t_val	DNS タイプ フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
t_val1 t_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージのすべてのセクション（質問および RR）を調べ、指定されたタイプを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS タイプに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
```

```
hostname(config-pmap)# match dns-type eq a
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match domain-name

DNS メッセージ ドメイン名リストに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match domain-name** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **domain-name regex** *regex_id*

match [**not**] **domain-name regex class** *class_id*

no match [**not**] **domain-name regex** *regex_id*

no match [**not**] **domain-name regex class** *class_id*

構文の説明

regex	正規表現を指定します。
regex_id	正規表現 ID を指定します。
class	複数の正規表現エントリが含まれているクラス マップを指定します。
class_id	正規表現クラス マップ ID を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、定義済みのリストと DNS メッセージのドメイン名を照合します。圧縮されたドメイン名は、照合の前に展開されます。一致条件は、他の DNS **match** コマンドと併用して、特定のフィールドにまで絞り込むことができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップで DNS ドメイン名を照合する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match domain-name regex
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dscp

クラス マップの（IP ヘッダーの）IETF-defined DSCP 値を識別するには、クラス マップ コンフィギュレーション モードで **match dscp** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match dscp {*values*}

no match dscp {*values*}

構文の説明

values	IP ヘッダーに最大 8 種類の IETF-defined DSCP 値を指定します。指定できる範囲は、0 ～ 63 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match dscp コマンドを使用すると、IP ヘッダーの IETF-defined DSCP 値を照合できます。

例

次に、クラス マップおよび **match dscp** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match dscp af43 cs1 ef
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match port	TCP/UDP ポートをそのインターフェイスで受信したパケットに対する比較基準として指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ehlo-reply-parameter

ESMTP ehlo reply パラメータに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match ehlo-reply-parameter** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **ehlo-reply-parameter** *parameter*

no match [**not**] **ehlo-reply-parameter** *parameter*

構文の説明

parameter	ehlo reply パラメータを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに ehlo reply パラメータに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match ehlo-reply-parameter auth
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filename

FTP 転送のファイル名に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filename** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション クラス マップに FTP 転送ファイル名に関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
hostname(config-cmap)# match username regex class ftp_regex_user
hostname(config-cmap)# match filename regex ftp-file
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filetype

FTP 転送のファイル タイプに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filetype** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション ポリシー マップに FTP 転送ファイルタイプに関して一致条件を設定する例を示します。

```
hostname(config-pmap)# match filetype class regex ftp-regex-filetype
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match flow ip destination-address

クラス マップにフロー IP 宛先アドレスを指定するには、クラス マップ コンフィギュレーション モードで **match flow ip destination-address** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match flow ip destination-address

no match flow ip destination-address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

トンネル グループに対するフローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** および **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併用します。フローを定義する基準は、宛先 IP アドレスです。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィックのクラス全体ではなく各フローに適用されます。QoS アクション ポリシーを適用するには、**match flow ip destination-address** コマンドを使用します。トンネル グループ内の各トンネルを指定されたレートに規制するには、**match tunnel-group** を使用します。

例

次の例では、トンネル グループ内でフローベースのポリシングをイネーブルにして、指定のレートに各トンネルを制限する方法を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	VPN の接続固有レコードを格納するデータベースを作成し、管理します。

match header

ESMTP ヘッダーに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match header** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

no match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

構文の説明

length gt *bytes*	ESMTP ヘッダー メッセージの長さを照合することを指定します。
line length gt bytes	ESMTP ヘッダー メッセージの 1 行の長さを照合することを指定します。
to-fields count gt *to_fields_number*	To: フィールドの数を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップにヘッダーに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match header length gt 512
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match header-flag

DNS ヘッダー フラグに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match header-flag** コマンドを使用します。設定されたヘッダー フラグを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

no match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

構文の説明

eq	完全一致を指定します。設定されていない場合は、**match-all** ビット マスク照合を指定します。
f_well_known	既知の名前で DNS ヘッダー フラグ ビットを指定します。複数のフラグ ビットを入力し、論理 OR を適用することもできます。 QR（Query、（注）QR=1、DNS 応答を示します） AA（Authoritative Answer） TC（TrunCation） RD（Recursion Desired） RA（Recursion Available）
f_value	任意の 16 ビット値を 16 進数形式で指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS クラス マップまたは DNS ポリシー マップで設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS ヘッダー フラグに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match header-flag AA
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match im-subscriber

SIP IM 加入者に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match im-subscriber** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次に、SIP インスペクション クラス マップに SIP IM 加入者に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match im-subscriber regex class im_sender
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match invalid-recipients

ESMTP 無効受信者アドレスに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match invalid-recipients** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **invalid-recipients count gt** *number*

no match [**not**] **invalid-recipients count gt** *number*

構文の説明

count gt *number*	無効な受信者数を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに無効な受信者数に関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match invalid-recipients count gt 1000
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ip address

指定されたいずれかのアクセス リストによって渡されるルート アドレスまたはマッチ パケットがあるルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ip address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match ip address {*acl...*}

no match ip address {*acl...*}

構文の説明

acl	アクセス リストの名前を指定します。複数のアクセス リストを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドはルート マップを削除します。

例

次の例では、内部ルートを再配布する方法を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。

コマンド	説明
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip next-hop

指定されたいずれかのアクセス リストによって渡されるネクストホップ ルータ アドレスがあるルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ip next-hop** コマンドを使用します。ネクスト ホップ エントリを削除するには、このコマンドの **no** 形式を使用します。

match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

no match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

構文の説明

acl	ACL の名前です。複数の ACL を指定できます。
prefix-list *prefix_list*	プレフィックス リストの名前です。

デフォルト

ルートは自由に配布されます。ネクストホップ アドレスを照合する必要はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コマンド構文に含まれる省略符号（...）は、コマンド入力に *acl* 引数の値を複数含めることができることを示します。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドはルート マップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートがルート マップを通過するようにするときには、ルート マップに複数の要素を持たせることができます。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、このルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

例

次に、アクセス リスト acl_dmz1 または acl_dmz2 によって渡されるネクストホップ ルータ アドレスがあるルートを配布する例を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip route-source

ACL に指定されているアドレスにあるルータおよびアクセス サーバによってアドバタイズされたルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ip route-source** コマンドを使用します。ネクスト ホップ エントリを削除するには、このコマンドの **no** 形式を使用します。

match ip route-source {*acl...*} | **prefix-list** *prefix_list*

no match ip route-source {*acl...*}

構文の説明

acl	ACL の名前です。複数の ACL を指定できます。
prefix_list	プレフィックス リストの名前です。

デフォルト

ルート送信元でのフィルタリングはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コマンド構文に含まれる省略符号（...）は、コマンド入力に access-list-name 引数の値を複数含めることができることを示します。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドはルート マップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルート マップは、いくつかの部分にわかれている可能性があります。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、このルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。ルートのネクストホップ アドレスと送信元ルータ アドレスが同じではない場合があります。

例

次に、acl_dmz1 および acl_dmz2 という ACL で指定されたアドレスにあるルータおよびアクセス サーバによってアドバタイズされたルートを配布する例を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかの ACL によって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match login-name

インスタント メッセージング用のクライアント ログイン名に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match login-name** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにクライアント ログイン名に関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match login-name regex login
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match media-type

H.323 メディア タイプに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match media-type** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **media-type [audio | data | video]**

no match [**not**] **media-type [audio | data | video]**

構文の説明

audio	オーディオ メディア タイプを照合することを指定します。
data	データ メディア タイプを照合することを指定します。
video	ビデオ メディア タイプを照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション クラス マップにオーディオ メディア タイプに関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match media-type audio
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message id

GTP メッセージ ID に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message id** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message id** [*message_id* | **range** *lower_range upper_range*]

no match [**not**] **message id** [*message_id* | **range** *lower_range upper_range*]

構文の説明

message_id	識別子を英数字 1 ～ 255 で指定します。
range *lower_range upper_range*	ID の下限と上限を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、GTP インスペクション クラス マップにメッセージ ID に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match message id 33
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message length

GTP メッセージ ID の一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message length** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message length min** *min_length* **max** *max_length*

no match [**not**] **message length min** *min_length* **max** *max_length*

構文の説明

min *min_length*	メッセージ ID の最小の長さを指定します。値の範囲は 1 ～ 65536 です。
max *max_length*	メッセージ ID の最大の長さを指定します。値の範囲は 1 ～ 65536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、GTP インスペクション クラス マップにメッセージの長さに関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match message length min 8 max 200
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message-path

Via ヘッダー フィールドの指定に従って SIP メッセージがたどるパスに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match message-path** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次の例では、SIP インスペクション クラス マップで SIP メッセージによって取得されるパスの一致条件を設定する方法を示します。

```
hostname(config-cmap)# match message-path regex class sip_message
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match mime

ESMTP MIME エンコーディング タイプ、MIME ファイル名の長さ、または MIME ファイル タイプに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match mime** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

no match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

構文の説明

encoding *type*	エンコーディング タイプを照合することを指定します。
filename length gt *bytes*	ファイル名の長さを照合することを指定します。
filetype *regex*	ファイル タイプを照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに MIME ファイル名の長さに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match mime filename length gt 255
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match peer-ip-address

インスタント メッセージングのピア IP アドレスに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match peer-ip-address** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **peer-ip-address** *ip_address ip_address_mask*

no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

構文の説明

ip_address	クライアントまたはサーバのホスト名または IP アドレスを指定します。
ip_address_mask	クライアントまたはサーバ IP アドレスのネットマスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにピア IP アドレスに関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match peer-login-name

インスタント メッセージングのピア ログイン名に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match peer-login-name** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにピア ログイン名に関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-login-name regex peerlogin
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match port

モジュラ ポリシー フレームワークを使用する場合、クラス マップ コンフィギュレーション モードで **match port** コマンドを使用して、アクションを適用する TCP ポートまたは UDP ポートを照合します。**match port** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

構文の説明

eq *port*	単一のポート名またはポート番号を指定します。
range *beg_port end_port*	ポート範囲の開始値および終了値を 1 ～ 65535 の範囲で指定します。
tcp	TCP ポートを指定します。
udp	UDP ポートを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力した後、**matchport** コマンドを入力してトラフィックを識別できます。また、**match access-list** コマンドなど **match** コマンドの別のタイプを入力できます（**class-map type management** コマンドだけが match port コマンドを許可します）。クラス マップには **match port** コマンドを 1 つだけ含めることができ、他のタイプの **match** コマンドとは組み合わせることができません。

2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、クラス マップおよび **match port** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 8080
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従ってトラフィックを照合します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match precedence

クラス マップに precedence 値を指定するには、クラス マップ コンフィギュレーション モードで **match precedence** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match precedence *value*

no match precedence *value*

構文の説明

value	最大 4 つの precedence 値をスペースで区切って指定します。指定できる範囲は、0 ～ 7 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

IP ヘッダーに TOS バイトで表される値を指定するには、**match precedence** コマンドを使用します。

例

次に、クラス マップおよび **match precedence** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match precedence 1
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match protocol

MSN や Yahoo などの特定のインスタント メッセージング プロトコルに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match protocol** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **protocol** {**msn-im** | **yahoo-im**}

no match [**not**] **protocol** {**msn-im** | **yahoo-im**}

構文の説明

msn-im	MSN インスタント メッセージング プロトコルを照合することを指定します。
yahoo-im	Yahoo インスタント メッセージング プロトコルを照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップに Yahoo インスタント メッセージング プロトコルに関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match protocol yahoo-im
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match question

DNS の質問またはリソース レコードに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match question** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match {**question** | {**resource-record answer** | **authority** | **additional**}}

no match {**question** | {**resource-record answer** | **authority** | **additional**}}

構文の説明

question	DNS メッセージの質問部分を指定します。
resource-record	DNS メッセージのリソース レコード部分を指定します。
answer	Answer RR セクションを指定します。
authority	Authority RR セクションを指定します。
additional	Additional RR セクションを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS ヘッダーを調べ、指定されたフィールドとマッチングします。また、他の DNS **match** コマンドと併用して、特定の質問または RR タイプのインスペクションを定義できます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS 質問に関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match question
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match req-resp

HTTP 要求と HTTP 応答の両方に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match req-resp** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **req-resp content-type mismatch**

no match [**not**] **req-resp content-type mismatch**

構文の説明

content-type	要求の受け入れタイプに対する応答でコンテンツ タイプを照合することを指定します。
mismatch	応答の content type フィールドが、要求の accept フィールドのいずれかの MIME タイプに一致する必要があることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、次のチェックを行うことができます。

- content-type ヘッダーの値がサポート対象コンテンツ タイプの内部リストにあることを確認します。
- ヘッダー content-type が、メッセージのデータまたはエンティティ本文の実際のコンテンツに一致することを確認します。
- HTTP 応答の content type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドと一致することを確認します。

上記のチェックに失敗した場合、セキュリティ アプライアンスは設定されたアクションを実行します。

次に、サポート対象コンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストのコンテンツ タイプの中には、メッセージの本文部分で確認できないように、対応する正規表現（magic number）がないものがあります。この場合、HTTP メッセージは許可されます。

例

次に、HTTP ポリシー マップで HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限する例を示します。

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# match req-resp content-type mismatch
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-command

特定の FTP コマンドを制限するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match request-command** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-command** *ftp_command* [*ftp_command...*]

no match [**not**] **request-command** *ftp_command* [*ftp_command...*]

構文の説明

ftp_command	制限する FTP コマンドを 1 つ以上指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション ポリシー マップに特定の FTP コマンドに関して一致条件を設定する例を示します。

```
hostname(config)# policy-map type inspect ftp ftp_map1
hostname(config-pmap)# match request-command stou
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-method

SIP メソッド タイプに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match request-method** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-method** *method_type*

no match [**not**] **request-method** *method_type*

構文の説明

method_type	RFC 3261 およびサポートされている拡張に従って、メソッド タイプを指定します。サポートされているメソッド タイプには、ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次の例では、SIP インスペクション クラス マップで SIP メッセージによって取得されるパスの一致条件を設定する方法を示します。

```
hostname(config-cmap)# match request-method ack
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request method

HTTP 要求に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match request method** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

no match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

構文の説明

built-in-regex	コンテンツ タイプ、方法、または転送エンコーディングの組み込みの正規表現を指定します。
class *class_map name*	正規表現タイプのクラス マップの名前を指定します。
regex *regex_name*	**regex** コマンドを使用して設定されている正規表現の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

表 20-1　組み込みの正規表現値

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

例

次に、「GET」メソッドまたは「PUT」メソッドで「www\.xyz.com/.*\.asp」または「www\.xyz[0-9][0-9]\.com」にアクセスしようとしている HTTP 接続を許可し、ロギングする HTTP インスペクション ポリシー マップを定義する例を示します。それ以外の URL/ メソッドの組み合わせは、サイレントに許可されます。

```
hostname(config)# regex url1 "www\.xyz.com/.*\.asp
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"
hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit
hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit
hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit
hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match route-type

指定されたタイプのルートを再配布するには、ルート マップ コンフィギュレーション モードで **match route-type** コマンドを使用します。ルート タイプ エントリを削除するには、このコマンドの **no** 形式を使用します。

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

構文の説明

local	ローカルに生成された BGP ルート。
internal	OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート
external	OSPF 外部ルートまたは EIGRP 外部ルート。
type-1	（任意）ルート タイプ 1 を指定します。
type-2	（任意）ルート タイプ 2 を指定します。
nssa-external	外部 NSSA を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドはルート マップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルート マップは、いくつかの部分にわかれている可能性があります。ルートが **route-map** コマンドに関係のあるどの match 句とも一致しない場合、このルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

OSPF の場合、**external type-1** キーワードはタイプ 1 外部ルートにのみ一致し、**external type-2** キーワードは type 2 外部ルートにのみ一致します。

例

次の例では、内部ルートを再配布する方法を示します。

```
hostname(config)# route-map name
hostname(config-route-map)# match route-type internal
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match rtp

クラス マップに偶数ポートの UDP ポート範囲を指定するには、クラス マップ コンフィギュレーション モードで **match rtp** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match rtp *starting_port range*

no match rtp *starting_port range*

構文の説明

starting_port	偶数 UDP 宛先ポートの下限を指定します。指定できる範囲は、2000 ～ 65535 です。
range	RTP ポートの範囲を指定します。指定できる範囲は、0 ～ 16383 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

RTP ポート（*starting_port* から *starting_port* に *range* を加えた値の範囲の偶数 UDP ポート番号）とマッチングするには、**match rtp** コマンドを使用します。

例

次に、クラス マップおよび **match rtp** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match rtp 20000 100
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match sender-address

ESMTP 送信者電子メール アドレスに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match sender-address** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **sender-address [length gt** *bytes* | **regex** *regex***]**

no match [**not**] **sender-address [length gt** *bytes* | **regex** *regex***]**

構文の説明

length gt *bytes*	送信者電子メール アドレスの長さを照合することを指定します。
regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ESMTP インスペクション ポリシー マップに長さが 320 文字を超える送信者電子メール アドレスに関して一致条件を設定する例を示します。

```
hostname(config-pmap)# match sender-address length gt 320
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match server

FTP サーバに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match server** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

セキュリティ アプライアンスは、FTP サーバに接続するときにログイン プロンプトの上方に表示される初期 220 サーバ メッセージに基づいて、サーバ名とマッチングします。220 サーバ メッセージには、行が複数含まれることがあります。サーバとのマッチングは、DNS を介して解決されるサーバ名の FQDN に基づきません。

例

次に、FTP インスペクション ポリシー マップに FTP サーバに関して一致条件を設定する例を示します。

```
hostname(config-pmap)# match server class regex ftp-server
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match service

特定のインスタント メッセージング サービスに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match service** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

no match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

構文の説明

chat	インスタント メッセージング チャット サービスを照合することを指定します。
file-transfer	インスタント メッセージング ファイル転送サービスを照合することを指定します。
games	インスタント メッセージング ゲーム サービスを照合することを指定します。
voice-chat	インスタント メッセージング音声チャット サービスを照合することを指定します。
webcam	インスタント メッセージング Web カメラ サービスを照合することを指定します。
conference	インスタント メッセージング会議サービスを照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにチャット サービスに関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match service chat
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match third-party-registration

第三者登録の要求者に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match third-party-registration** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

third-party registration match コマンドは、SIP 登録または SIP プロキシで他のユーザを登録できるユーザを特定するために使用されます。From と To の値が一致しない場合には、REGISTER メッセージの From ヘッダー フィールドで識別されます。

例

次に、SIP インスペクション クラス マップに第三者登録に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match third-party-registration regex class sip_regist
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match tunnel-group

以前に定義したトンネル グループに属するクラス マップのトラフィックとマッチングするには、クラス マップ コンフィギュレーション モードで **match tunnel-group** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match tunnel-group *name*

no match tunnel-group *name*

構文の説明

name	トンネル グループ名のテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

match コマンドは、クラス マップのトラフィック クラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラス マップに含まれるトラフィックを定義するさまざまな基準が含まれています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

フローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** コマンドおよび **match tunnel-group** コマンドを **class-map**、**policy-map**、**service-policy** の各コマンドと併用します。フローを定義する基準は、宛先 IP アドレスです。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィックのクラス全体ではなく各フローに適用されます。QoS アクション ポリシーを適用するには、**police** コマンドを使用します。トンネル グループ内の各トンネルを指定されたレートに規制するには、**match tunnel-group** を **match flow ip destination-address** と併用します。

例

次の例では、トンネル グループ内でフローベースのポリシングをイネーブルにして、指定のレートに各トンネルを制限する方法を示します。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	IPSec および L2TP の接続固有レコードのデータベースを作成および管理します。

match uri

SIP ヘッダーの URI に関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match uri** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

no match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

構文の説明

sip	SIP URI を指定します。
tel	TEL URI を指定します。
length gt *gt_bytes*	URI の最大長を指定します。値の範囲は、0 ～ 65536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次に、SIP メッセージの URI に関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match uri sip length gt
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match url-filter

RTSP メッセージの URL フィルタリングに関して一致条件を設定するには、クラス マップまたはポリシー マップ コンフィギュレーション モードで **match url-filter** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RTSP クラス マップまたはポリシー マップで設定できます。

例

次に、RTSP インスペクション ポリシー マップに URL フィルタリングに関して一致条件を設定する例を示します。

```
hostname(config)# regex badurl www.url1.com/rtsp.avi
hostname(config)# policy-map type inspect rtsp rtsp-map
hostname(config-pmap)# match url-filter regex badurl
hostname(config-pmap-p)# drop-connection
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match username

FTP ユーザ名に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match username** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション クラス マップに FTP ユーザ名に関して一致条件を設定する例を示します。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# match username regex class ftp_regex_user
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match version

GTP メッセージ ID の一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message length** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

構文の説明

vresion_id	バージョンを 0 ～ 255 の範囲で指定します。
range *lower_range upper_range*	バージョンの下限および上限を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップで設定できます。GTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、GTP インスペクション クラス マップにメッセージ バージョンに関して一致条件を設定する例を示します。

```
hostname(config-cmap)# match version 1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

max-failed-attempts

サーバ グループの特定のサーバが非アクティブ化されるまでに、そのサーバに対して許可されている試行の失敗数を指定するには、AAA サーバ グループ コンフィギュレーション モードで **max-failed-attempts** コマンドを使用します。この指定を削除し、デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

max-failed-attempts *number*

no max-failed-attempts

構文の説明

number	前述の **aaa-server** コマンドに指定されているサーバ グループの特定のサーバに対して許可されている接続試行の失敗数を指定する 1 ～ 5 の範囲の整数。

デフォルト

number のデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA-server グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行する前に、AAA サーバ/グループを設定しておく必要があります。

例

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 4
hostname(config-aaa-server-group)#
```

関連コマンド

コマンド	説明
aaa-server *server-tag* **protocol** *protocol*	AAA サーバ グループ コンフィギュレーション モードを開始して、グループ内のすべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できるようにします。

clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

max-forwards-validation

Max-forwards ヘッダー フィールドが 0 かどうかのチェックをイネーブルにするには、パラメータ コンフィギュレーション モードで **max-forwards-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

no max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、宛先へのホップの数をカウントします。宛先に達する前に 0 になることができません。

例

次に、SIP インスペクション ポリシー マップに最大転送数の検証をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# max-forwards-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

max-header-length

HTTP ヘッダーの長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **max-header-length** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
request	要求メッセージ。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。
response	（任意）応答メッセージ。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-header-length コマンドをイネーブルにすると、セキュリティ アプライアンスは設定された制限内の HTTP ヘッダーがあるメッセージのみを許可し、そのようなヘッダーがない場合には指定されたアクションを実行します。セキュリティ アプライアンスが TCP 接続をリセットし、任意で syslog エントリを作成するようにするには、**action** キーワードを使用します。

例

次に、HTTP 要求を HTTP ヘッダーが 100 バイトを超えない要求に制限する例を示します。ヘッダーが大きすぎる場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

max-object-size

WebVPN セッションに対してセキュリティ アプライアンスがキャッシュできるオブジェクトの最大サイズを設定するには、キャッシュ モードで max-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。

max-object-size *integer range*

構文の説明

integer range	0 ～ 10000 KB

デフォルト

1000 KB

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

最大オブジェクト サイズは、最小オブジェクト サイズよりも大きい値である必要があります。キャッシュ圧縮がイネーブルになっている場合、セキュリティ アプライアンスは、オブジェクトを圧縮してからサイズを計算します。

例

次に、最大オブジェクト サイズを 4000 KB に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# max-object-size 4000
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

max-retry-attempts

要求がタイムアウトされるまでにセキュリティ アプライアンスが失敗した SSO 認証を再試行できる回数を設定するには、特定の SSO サーバ タイプの webvpn コンフィギュレーション モードで **max-retry-attempts** コマンドを使用します。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

max-retry-attempts *retries*

no max-retry-attempts

構文の説明

retries	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数 指定できる範囲は 1 ～ 5 回です。

デフォルト

このコマンドのデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

いったん SSO 認証をサポートするようにセキュリティ アプライアンスを設定すると、任意で 2 つのタイムアウト パラメータを調整できます。

- **max-retry-attempts** コマンドを使用してセキュリティ アプライアンスが失敗した SSO 認証を再試行できる回数。
- 失敗した SSO 認証がタイムアウトするまでの秒数（**request-timeout** コマンドを参照）。

例

次に、webvpn-sso-siteminder コンフィギュレーション モードを開始し、my-sso-server という名前の SiteMinder SSO サーバ名に対する認証再試行を 4 つ設定する例を示します。

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
```

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

max-uri-length

HTTP 要求メッセージの URI の長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **max-uri-length** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-uri-length コマンドをイネーブルにすると、セキュリティ アプライアンスは設定された制限内の URI があるメッセージのみを許可し、そのような URI がない場合には指定されたアクションを実行します。セキュリティ アプライアンスに TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

長さが設定された値以下の URI が許可されます。それ以外の場合には、指定されたアクションが実行されます。

例

次に、HTTP 要求を URI が 100 バイトを超えない要求に制限する例を示します。URI が大きすぎる場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

mcc

IMSI プレフィックス フィルタリングのモバイル国コードおよびモバイル ネットワーク コードを識別するには、GTP マップ コンフィギュレーション モードで **mcc** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

構文の説明

country_code	モバイル国コードを識別するゼロ以外の 3 桁の値。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
network_code	ネットワーク コードを識別する 2 桁または 3 桁の値。

デフォルト

デフォルトでは、セキュリティ アプライアンスは有効な MCC/MNC の組み合わせをチェックしません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IMSI プレフィックス フィルタリングに使用されます。受信パケットの IMSI の MCC および MNC は、このコマンドで設定された MCC および MNC と比較され、一致しない場合はドロップされます。

このコマンドは、IMSI プレフィックス フィルタリングをイネーブルにするために使用する必要があります。複数のインスタンスを設定して許可する MCC と MNC の組み合わせを指定できます。デフォルトでは、セキュリティ アプライアンスは MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次に、MCC を 111、MNC を 222 として、IMSI プレフィックス フィルタリングのトラフィックを識別する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

media-termination address

IP アドレスを電話プロキシ機能へのメディア接続に使用するように指定するには、電話プロキシ コンフィギュレーション モードで **media-termination address** コマンドを使用します。

電話プロキシ コンフィギュレーションからメディア ターミネーション アドレスを削除するには、このコマンドの **no** 形式を使用します。

media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

no media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

構文の説明

ip_address	電話プロキシでメディア終端時に使用できるように作成する仮想 IP アドレスを指定します。電話プロキシのインスタンスごとに設定できる仮想インターフェイスは 1 つのみです。ASA 電話プロキシは、シグナリング メッセージのメディア アドレス部分にメディア終端 IP アドレスを挿入します。
rtp-max-port *port2*	メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。*port2* には、32767 ～ 65535 の値を指定できます。
rtp-min-port *port1*	メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。*port1* には、1024 ～ 16384 の値を指定できます。

デフォルト

デフォルトで、**rtp-min-port** キーワードの *port1* の値は 16384、**rtp-max-port** キーワードの *port2* の値は 32767 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
電話プロキシ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

セキュリティ アプライアンスには、次の基準を満たすメディア終端の IP アドレスが必要です。

- IP アドレスは、ネットワーク上の別のデバイスによって使用されることがなく、セキュリティ アプライアンスインターフェイスに接続されたネットワーク上にある未使用の IP アドレスである、パブリックにルーティング可能な IP アドレスです。
- セキュリティ アプライアンスインターフェイス IP アドレスと同じ IP アドレスを指定することはできません。特に、セキュリティ アプライアンスでセキュリティ レベルが最も低いインターフェイスと同じにすることはできません。
- IP アドレスは、既存のスタティック NAT 規則と重複できません。

- IP アドレスは、CUCM または TFTP サーバの IP アドレスと同じにはできません。
- 他のインターフェイスの IP 電話がメディア終端アドレスに到達できるように、他のインターフェイスにルートを追加します。

電話プロキシでサポートするコール数の規模を調整する必要がある場合は、メディア ターミネーション ポイントの RTP ポート範囲を設定します。

例

次に、**media-termination address** コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
hostname(config-phone-proxy)# media-termination address 192.168.1.4
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

media-type

メディア タイプを銅線またはファイバ ギガビット イーサネットに設定するには、インターフェイス コンフィギュレーション モードで **media-type** コマンドを使用します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの 4GE SSM でファイバ SFP コネクタが使用可能になります。メディア タイプ設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

media-type {**rj45** | **sfp**}

no media-type [**rj45** | **sfp**]

構文の説明

rj45	（デフォルト）メディア タイプを銅線 RJ-45 コネクタに設定します。
sfp	メディア タイプをファイバ SFP コネクタに設定します。

デフォルト

デフォルトは **rj45** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0（4）	このコマンドが導入されました。

使用上のガイドライン

sfp 設定は、固定速度（1000 Mbps）を使用するため、**speed** コマンドを使用すると、インターフェイスがリンク パラメータをネゴシエートするかどうかを設定できます。**duplex** コマンドは、**sfp** ではサポートされません。

例

次に、メディア タイプを SFP に設定する例を示します。

```
hostname(config)# interface gigabitethernet1/1
hostname(config-if)# media-type sfp
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

member

コンテキストをリソース クラスに割り当てるには、コンテキスト コンフィギュレーション モードで **member** コマンドを使用します。コンテキストをリソース クラスから削除するには、このコマンドの **no** 形式を使用します。

member *class_name*

no member *class_name*

構文の説明

class_name	**class** コマンドで作成したクラス名を指定します。

デフォルト

デフォルトでは、コンテキストはデフォルトのクラスに割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストがセキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

例

次に、コンテキスト テストをゴールド クラスに割り当てる例を示します。

```
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
limit-resource	リソースの制限を設定します。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

member-interface

物理インターフェイスを冗長インターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **member-interface** コマンドを使用します。このコマンドは、冗長インターフェイス タイプでのみ使用できます。2 つのメンバ インターフェイスを冗長インターフェイスに割り当てることができます。メンバ インターフェイスを削除するには、このコマンドの **no** 形式を使用します。冗長インターフェイスから両方のメンバ インターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバ インターフェイスが必要です。

member-interface *physical_interface*

no member-interface *physical_interface*

構文の説明

physical_interface	**gigabitethernet0/1** などのインターフェイス ID を識別します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。

名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。この場合、まず **no nameif** コマンドを使用して名前を削除する必要があります。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

冗長インターフェイス ペアの一部である物理インターフェイスに使用できるコンフィギュレーションのみが物理パラメータ（**speed** コマンド、**duplex** コマンド、**description** コマンド、**shutdown** コマンドなど）です。また、**default** や **help** などの実行時コマンドを入力することもできます。

アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

アクティブ インターフェイスを変更するには、**redundant-interface** コマンドを入力します。

冗長インターフェイスは、最初に追加された物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、メンバー インターフェイスの MAC アドレスとは関係なく使用される MAC アドレスを冗長インターフェイスに割り当てることができます（**mac-address** コマンドまたは **mac-address auto** コマンドを参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合は、同じ MAC アドレスが維持されるため、トラフィックが妨げられることはありません。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
redundant-interface	アクティブなメンバ インターフェイスを変更します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

memberof

このユーザがメンバであるグループ名のリストを指定するには、ユーザ名属性コンフィギュレーション モードで **memberof** コマンドを使用します。この属性をコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

memberof *group_1*[,*group_2,...group_n*]

[**no**] **memberof** *group_1*[,*group_2,...group_n*]

構文の説明

group_1 through group_n	このユーザが所属するグループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このユーザが所属するグループ名のカンマ区切りリストを入力します。

例

次に、グローバル コンフィギュレーション モードを開始し、ユーザ名を newuser という名前で作成し、newuser が DevTest グループおよび管理グループのメンバであることを指定する例を示します。

```
hostname(config)# username newuser nopassword
hostname(config)# username newuser attributes
hostname(config-username)# memberof DevTest,management
hostname(config-username)#
```

関連コマンド

コマンド	説明
clear configure username	ユーザ名データベース全体または指定されたユーザ名のみをクリアします。

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザに対して現在実行されているユーザ コンフィギュレーションを表示します。
username	ユーザ名のデータベースを作成および管理します。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールをイネーブルにするには、特権 EXEC モードで **memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールをディセーブルにするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによってメモリが解放された後、解放メモリの変化をモニタできます。

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

memory delayed-free-poisoner enable コマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに大きな影響を及ぼします。このコマンドは、Cisco TAC の指導の下でのみ使用する必要があります。システムの使用率が高い間は、実働環境では実行しないでください。

このツールをイネーブルにすると、セキュリティ アプライアンスで実行されているアプリケーションによるメモリ解放要求が FIFO キューに書き込まれます。要求がキューに書き込まれるたびに、それに伴うメモリ バイトのうち、下位メモリ管理には必要ないバイトが、値 0xcc で書き込まれて「改ざん」されます。

メモリ解放要求は、空きメモリ プールにある量よりも多くのメモリがアプリケーションで必要になるまで、キューに残ります。メモリが必要になると、最初のメモリ解放要求がキューから取り出され、改ざんされたメモリが検証されます。

メモリに変更がない場合、メモリは下位メモリ プールに返され、ツールは最初に要求を行ったアプリケーションからのメモリ要求を再発行します。この処理は、要求元のアプリケーションに十分なメモリが解放されるまで続きます。

改ざんされたメモリに変更があった場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。また、**memory delayed-free-poisoner validate** コマンドを使用して、検証を手動で開始できます。

このコマンドの **no** 形式は、要求で参照されるキュー内のすべてのメモリを検証なしで空きメモリ プールに返し、統計カウンタをクリアします。

例

次に、delayed free-memory poisoner ツールをイネーブルにする例を示します。

```
hostname# memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再利用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

表 20-2 に、出力の重要な部分を示します。

表 20-2　不正なメモリ使用に関する出力の説明

フィールド	説明
heap region	要求元のアプリケーションが使用できるメモリ領域のアドレス領域およびサイズ。これは、要求されたサイズと同じ値ではなく、メモリ要求が行われたときにシステムがメモリを配分できるように小さくなることがあります。
memory address	障害が検出されたメモリの位置。
byte offset	バイト オフセットはヒープ領域の先頭を基準にしており、このアドレスから始まるデータ構造を保持するためにフィールドが変更された場合には、バイト オフセットを使用してそのフィールドを見つけることができます。値が 0 か、またはヒープ領域バイト カウントよりも大きい値である場合は、問題が下位ヒープ パッケージの予期しない値であることを示している可能性があります。
allocated by/freed by	この特定のメモリ領域に関して実施された最後の malloc/calloc/realloc および解放要求の命令アドレス。
Dumping...	検出された障害がヒープ メモリ領域の先頭にどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーに続く 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュとキュー リンクを保持するために使用するメモリです。システム ヒープ トレーラが検出されるまでの領域内のそれ以外のバイトは、0xcc に設定する必要があります。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キューのすべての要素を強制的に検証するには、特権 EXEC モードで **memory delayed-free-poisoner validate** コマンドを使用します。

memory delayed-free-poisoner validate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

memory delayed-free-poisoner validate コマンドを発行する場合は、事前に **memory delayed-free-poisoner enable** コマンドを使用して delayed free-memory poisoner ツールをイネーブルにする必要があります。

memory delayed-free-poisoner validate コマンドにより、**memory delayed-free-poisoner** キューの各要素が検証されます。要素に予期しない値が含まれている場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。予期しない値がない場合、要素はキューに残り、ツールによって正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステム メモリ プールに返されません。

（注） delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。

例

次に、**memory delayed-free-poisoner** キューのすべての要素を検証する例を示します。

```
hostname# memory delayed-free-poisoner validate
```

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory caller-address

コール トレースまたは発信元 PC 用にプログラム メモリの特定の範囲を設定して、メモリの問題を容易に特定できるようにするには、特権 EXEC モードで **memory caller-address** コマンドを使用します。発信元 PC は、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス範囲を削除するには、このコマンドの **no** 形式を使用します。

memory caller-address *startPC endPC*

no memory caller-address

構文の説明

endPC	メモリ ブロックの終了アドレス範囲を指定します。
startPC	メモリ ブロックの開始アドレス範囲を指定します。

デフォルト

メモリを追跡できるように、実際の発信元 PC が記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

メモリの問題を特定のメモリ ブロックに限定するには、**memory caller-address** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信元 PC が、プログラムの多くの場所で使用されている既知のライブラリ関数であることがあります。プログラムの個々の場所を特定するには、そのライブラリ関数の開始プログラム アドレスおよび終了プログラム アドレスを設定し、それによってライブラリ関数の呼び出し元のプログラム アドレスを記録します。

（注） 発信元アドレスの追跡をイネーブルにすると、セキュリティ アプライアンスのパフォーマンスが一時的に低下することがあります。

例

次に、**memory caller-address** コマンドで設定したアドレス範囲、および **show memory-caller address** コマンドによる表示結果の例を示します。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464
```

```
hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレス範囲を表示します。

memory profile enable

メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにするには、特権 EXEC モードで **memory profile enable** コマンドを使用します。メモリのプロファイルリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

構文の説明

peak_value	メモリ使用状況のスナップショットを使用率ピーク バッファに保存するメモリ使用状況しきい値を指定します。このバッファの内容を後で分析して、システムのピーク時のメモリ ニーズを判断できます。

デフォルト

デフォルトでは、メモリ プロファイリングはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

メモリ プロファイリングをイネーブルにする前に、**memory profile text** コマンドを使用して、プロファイリングするメモリ テキスト範囲を設定する必要があります。

clear memory profile コマンドを入力するまで、一部のメモリはプロファイリング システムによって保持されます。**show memory status** コマンドの出力を参照してください。

（注） メモリ プロファイリングをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスが一時的に低下する場合があります。

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
hostname# memory profile enable
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。

memory profile text

プロファイリングするメモリのプログラム テキスト範囲を設定するには、特権 EXEC モードで **memory profile text** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

構文の説明

all	メモリ ブロックのテキスト範囲全体を指定します。
endPC	メモリ ブロックの終了テキスト範囲を指定します。
resolution	ソース テキスト領域の追跡精度を指定します。
startPC	メモリ ブロックの開始テキスト範囲を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

テキスト範囲が小さい場合、精度を「4」にすると、命令への呼び出しが正常に追跡されます。テキスト範囲が大きい場合、精度を粗くしても初回通過には十分であり、範囲は次回の通過でさらに小さな領域にまで絞り込むことができます。

メモリ プロファイリングを開始するには、**memory profile text** コマンドでテキスト範囲を入力した後、続けて **memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

（注） メモリ プロファイリングをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスが一時的に低下する場合があります。

例

次に、精度を 4 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

```
hostname# memory profile text 0x004018b4 0x004169d0 4
```

次に、メモリ プロファイリングのテキスト範囲のコンフィギュレーションおよびステータス（OFF）を表示する例を示します。

```
hostname# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

（注）　メモリ プロファイリングを開始するには、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

関連コマンド

コマンド	説明
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレス範囲を表示します。

memory-size

WebVPN のさまざまなコンポーネントがアクセスできるセキュリティ アプライアンス上のメモリ容量を設定するには、webvpn モードで **memory-size** コマンドを使用します。設定されたメモリ容量（KB 単位）または合計メモリの割合として、メモリ容量を設定できます。設定されたメモリ サイズを削除するには、このコマンドの **no** 形式を使用します。

（注） 新しいメモリ サイズ設定を有効にするには、リブートが必要です。

memory-size {percent | kb} *size*

no memory-size [{percent | kb} *size***]**

構文の説明

kb	メモリ容量をキロバイト単位で指定します。
percent	セキュリティ アプライアンス上のメモリ容量を合計メモリの割合として指定します。
size	メモリ容量を KB 単位または合計メモリの割合として指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

設定したメモリ容量は、ただちに割り当てられます。このコマンドを設定する前に、show memory を使用して、使用可能なメモリ容量を確認してください。設定に合計メモリの割合を使用する場合は、設定した値が使用可能な割合を下回っていることを確認してください。設定にキロバイトの値を使用する場合は、設定した値がキロバイト単位の使用可能なメモリ容量を下回っていることを確認してください。

例

次に、WebVPN メモリ サイズを 30 % に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# memory-size percent 30
hostname(config-webvpn)#
hostname(config-webvpn)# reload
```

コマンド	説明
show memory webvpn	WebVPN メモリ使用状況の統計情報を表示します。

memory tracking enable

ヒープ メモリ要求の追跡をイネーブルにするには、特権 EXEC モードで **memory tracking enable** コマンドを使用します。メモリ追跡をディセーブルにするには、このコマンドの **no** 形式を使用します。

memory tracking enable

no memory tracking enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0（8）	このコマンドが導入されました。

使用上のガイドライン

ヒープ メモリ要求を追跡するには、**memory tracking enable** コマンドを使用します。メモリ追跡をディセーブルにするには、このコマンドの **no** 形式を使用します。

例

次に、ヒープ メモリ要求の追跡をイネーブルにする例を示します。

```
hostname# memory tracking enable
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。
show memory tracking	現在割り当てられているメモリを表示します。
show memory tracking address	ツールの追跡対象である現在割り当てられている各メモリのサイズ、位置、および最上位呼び出し元関数を一覧表示します。
show memory tracking dump	このコマンドは、指定されたメモリ アドレスのサイズ、位置、呼び出しスタックの一部、およびメモリ ダンプを表示します。
show memory tracking detail	ツール内部の動作の洞察に使用されるさまざまな内部詳細情報を表示します。

merge-dacl

ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL をマージするには、AAA サーバ グループ コンフィギュレーション モードで **merge-dacl** コマンドを使用します。ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL のマージをディセーブルにするには、このコマンドの **no** 形式を使用します。

merge dacl {**before_avpair** | **after_avpair**}

no merge dacl

構文の説明

after_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペアのエントリの後に配置する必要があることを指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および セキュリティ アプライアンス で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL が結合されているどうかを判断します。セキュリティ アプライアンス で設定される ACL には適用されません。
before_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペア のエントリの前に配置する必要があることを指定します。

デフォルト

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA-server グループ コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

AV ペアおよびダウンロード可能な ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

例

次の例では、ダウンロード可能 ACL のエントリが Cisco AV ペアのエントリの前に配置されるように指定しています。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

関連コマンド

コマンド	説明
aaa-server host	サーバと、そのサーバが属する AAA サーバ グループを識別します。
aaa-server protocol	サーバ グループ名とプロトコルを識別します。
max-failed-attempts	次のサーバを試す前に、グループ内の AAA サーバに送信する要求の最大数を指定します。

message-length

設定された最大および最小の長さを満たさない GTP パケットをフィルタリングするには、GTP マップ コンフィギュレーション モードで **message-length** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。コマンドを削除するには、**no** 形式を使用します。

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

構文の説明

max	UDP ペイロードに許可されている最大バイト数を指定します。
max_bytes	UDP ペイロード内の最大バイト数。範囲は、1 ～ 65,536 です。
min	UDP ペイロードに許可されている最少バイト数を指定します。
min_bytes	UDP ペイロード内の最小バイト数。範囲は、1 ～ 65,536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定する長さは、GTP ヘッダーとメッセージの残りの部分（UDP パケットのペイロード）の合計です。

例

次に、長さが 20 ～ 300 バイトのメッセージを許可する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

mfib forwarding

インターフェイスで MFIB 転送を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** を使用します。インターフェイスで MFIB 転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

mfib forwarding

no mfib forwarding

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの MFIB 転送をイネーブルにします

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト ルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで MFIB 転送がイネーブルになります。特定のインターフェイスで MFIB 転送をディセーブルにするには、このコマンドの **no** 形式を使用します。実行コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

インターフェイスで MFIB 転送がディセーブルになっている場合、特に他の方法を設定しない限り、そのインターフェイスはマルチキャスト パケットを受け付けません。MFIB 転送がディセーブルになっていると、IGMP パケットも阻止されます。

例

次に、指定されたインターフェイスで MFIB 転送をディセーブルにする例を示します。

```
hostname(config)# interface GigabitEthernet 0/0
hostname(config-if)# no mfib forwarding
```

関連コマンド

コマンド	説明
multicast-routing	マルチキャスト ルーティングをイネーブルにします。
pim	インターフェイス上の PIM をイネーブルにします。

min-object-size

WebVPN セッションに対してセキュリティ アプライアンスがキャッシュできるオブジェクトの最小サイズを設定するには、キャッシュ モードで min-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。最小オブジェクト サイズを設定しないようにするには、値にゼロ（0）を入力します。

min-object-size *integer range*

構文の説明

integer range	0 ～ 10000 KB。

デフォルト

デフォルトのサイズは 0 KB です。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

最小オブジェクト サイズは、最大オブジェクト サイズよりも小さい値である必要があります。キャッシュ圧縮がイネーブルになっている場合、セキュリティ アプライアンスは、オブジェクトを圧縮してからサイズを計算します。

例

次に、最大オブジェクト サイズを 40 KB に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# min-object-size 40
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。

コマンド	説明
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。

mkdir

新規ディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	作成するディレクトリの名前およびパス。

デフォルト

パスを指定しないと、現在の作業ディレクトリにディレクトリが作成されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

同じ名前のディレクトリがすでに存在する場合、新規のディレクトリは作成されません。

例

次の例は、「backup」という新しいディレクトリを作成する方法を示しています。

```
hostname# mkdir backup
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
rmdir	指定されたディレクトリを削除します。
pwd	現在の作業ディレクトリを表示します。

mode

セキュリティ コンテキスト モードを single または multiple に設定するには、グローバル コンフィギュレーション モードで **mode** コマンドを使用します。1 つの セキュリティ アプライアンス をいくつかのパーティションに分けて複数の仮想デバイス（セキュリティ コンテキストと呼びます）に配置できます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティ ポリシー、インターフェイス、および管理者で構成されています。複数のコンテキストが存在することは、複数のスタンドアロン アプライアンスが設置されていることと同じです。シングル モードでは、セキュリティ アプライアンスはシングル コンフィギュレーションを備え、単一デバイスとして動作します。マルチ モードでは、複数のコンテキストを作成し、それぞれに独自のコンフィギュレーションを設定できます。許可されるコンテキストの数は、保有するライセンスによって異なります。

mode {**single** | **multiple**} [**noconfirm**]

構文の説明

multiple	マルチ コンテキスト モードを設定します。
noconfirm	（任意）ユーザに確認を求めることなく、モードを設定します。このオプションは自動スクリプトで役立ちます。
single	コンテキスト モードを single に設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、セキュリティ アプライアンスに各コンテキストのコンフィギュレーションが含まれ、それぞれのコンフィギュレーションでは、スタンドアロン デバイスに設定できるセキュリティ ポリシー、インターフェイス、およびほぼすべてのオプションが識別されます（コンテキスト コンフィギュレーションの場所を識別するには、**config-url** コマンドを参照してください）。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、セキュリティ アプライアンス の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

mode コマンドを使用してコンテキスト モードを変更すると、再起動するように求められます。

コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、**mode** コマンドを使用して、新規デバイスのモードを match に設定します。

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンスは実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。セキュリティ アプライアンス は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

マルチ モードからシングル モードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）をセキュリティ アプライアンスにコピーすることを推奨します。マルチ モードから継承されるシステム コンフィギュレーションは、シングル モード デバイスで完全に機能するコンフィギュレーションではありません。

マルチ コンテキスト モードのすべての機能がサポートされるわけではありません。詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、モードを multiple に設定する例を示します。

```
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

次に、モードを single に設定する例を示します。

```
hostname(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....
```

```
Booting system, please wait...
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

monitor-interface

特定のインターフェイスでヘルス モニタリングをイネーブルにするには、グローバル コンフィギュレーション モードで **monitor-interface** コマンドを使用します。インターフェイスのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

monitor-interface *if_name*

no monitor-interface *if_name*

構文の説明

if_name	モニタするインターフェイスの名前を指定します。

デフォルト

物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス用にモニタできるインターフェイスの数は 250 です。インターフェイス ポーリング頻度ごとに、セキュリティ アプライアンス フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。

モニタ対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

アクティブ/アクティブ フェールオーバーでは、このコマンドはコンテキスト内でだけ有効です。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにしています。

```
hostname(config)# monitor-interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure monitor-interface	すべてのインターフェイスでデフォルトのインターフェイス ヘルス モニタリングに戻します。
failover interface-policy	モニタするインターフェイスの数または割合を指定します。モニタの対象となるのは、障害が発生すると、フェールオーバーが発生するインターフェイスです。
failover polltime	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Standby フェールオーバー）。
polltime interface	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Active フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、**more** コマンドを使用します。

more {**/ascii** | **/binary**| **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:**}*filename*

構文の説明

/ascii	（任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。
/binary	（任意）任意のファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
disk0*:*	（任意）内部フラッシュ メモリのファイルを表示します。
disk1:	（任意）外部フラッシュ メモリ カードのファイルを表示します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
ftp:	（任意）FTP サーバ上のファイルを表示します。
http:	（任意）Web サイトのファイルを表示します。
https:	（任意）セキュア Web サイトのファイルを表示します。
system:	（任意）ファイル システムを表示します。
tftp:	（任意）TFTP サーバ上のファイルを表示します。
filename	表示するファイルの名前を指定します。

デフォルト

ASCII モード

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

more filesystem: コマンドは、ローカル ディレクトリまたはファイル システムのエイリアスを入力するように求めます。

例

次の例は、「test.cfg」という名前のローカル ファイルの内容を表示する方法を示しています。

```
hostname# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
```

```
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

コマンド	説明
cd	指定されたディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

mount（CIFS）

セキュリティ アプライアンスから Common Internet File System（CIFS; 共通インターネット ファイル システム）にアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount** コマンドを使用します。このコマンドを使用すると、設定マウント cifs コンフィギュレーション モードを開始できます。CIFS ネットワーク ファイル システムをマウント解除するには、このコマンドの **no** 形式を使用します。

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

構文の説明

domain *domain-name*	（任意）CIFS ファイル システムでのみ、この引数には Windows NT ドメイン名を指定します。最大 63 文字が許可されます。
name	ローカル CA に割り当てられる既存のファイル システムの名前を指定します。
no	すでにマウント済みの CIFS ファイル システムを削除し、アクセスできないようにします。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
server *server-name*	CIFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
share *sharename*	サーバ内のファイル データにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
status enable/disable	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
type	マウントするファイル システムの CIFS タイプを指定します。代替の **type** キーワードについては、**mount（FTP）**コマンドを参照してください。
type cifs	マウントされるファイル システムが CIFS であることを指定します。CIFS は、CIFS 共有ディレクトリにボリューム マウント機能を提供するファイル システムです。
user *username*	ファイル システムのマウントが認可されているユーザ名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
設定マウント cifs コンフィギュレーション	•	•	•	—	•
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

mount コマンドは、Installable File System（IFS）を使用して、CIFS ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

mount コマンドは、セキュリティ アプライアンス上の CIFS ファイル システムを UNIX ファイル ツリーにアタッチします。逆に、**no mount** コマンドはそのアタッチを解除します。

mount コマンドに指定されている *mount-name* は、セキュリティ アプライアンスにすでにマウントされているファイル システムを参照するために、他の CLI コマンドで使用されます。たとえば、ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

CIFS リモート ファイル アクセス プロトコルは、アプリケーションがローカル ディスクおよびネットワーク ファイル サーバ上のデータを共有する方法と互換性があります。TCP/IP を運用し、インターネットのグローバル DNS を使用する CIFS は、Windows オペレーティング システムにネイティブのファイル共有プロトコルである Microsoft のオープンでクロス プラットフォームの Server Message Block（SMB; サーバ メッセージ ブロック）プロトコルを拡張したものです。

mount コマンドを使用した後は、必ずルート シェルを終了してください。mount-cifs-config モードの **exit** キーワードは、ユーザをグローバル コンフィギュレーション モードに戻します。

再接続するには、接続をストレージに再マッピングします。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています （**mount** *name* **type ftp** コマンドを参照）。Network File System（NFS; ネットワーク ファイル システム）ボリュームのマウントは、このリリースではサポートされていません。

例

次に、*cifs://amer;chief:big-boy@myfiler02/my_share* を *cifs_share* というラベルとしてマウントする例を示します。

```
hostname(config)# mount cifs_share type CIFS
hostname (config-mount-cifs)# server myfiler02a
```

関連コマンド

コマンド	説明
debug cifs	CIFS デバッグ メッセージをロギングします。
debug ntdomain	Web VPN NT ドメイン デバッグ メッセージをロギングします。
debug webvpn cifs	WebVPN CIFS デバッグ メッセージをロギングします。
dir all-filesystems	セキュリティ アプライアンスにマウントされているすべてのファイル システムのファイルを表示します。

mount（FTP）

セキュリティ アプライアンスからファイル転送プロトコル（FTP）ファイル システムにアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount** *name* **type ftp** コマンドを使用して、マウント FTP コンフィギュレーション モードを開始します。**no mount** *name* **type ftp** コマンドは、FTP ネットワーク ファイル システムをマウント解除するために使用されます。

[**no**] **mount** *name* **type FTP server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

構文の説明

exit	Mount-FTP コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。
ftp	マウントされるファイル システムが FTP であることを指定します。FTP は Linux カーネル モジュールであり、FTP 共有ディレクトリをマウントできるようにする FTP ボリューム マウント機能で Virtual File System（VFS; 仮想ファイル システム）を拡張したものです。
mode	FTP 転送モードをアクティブまたはパッシブとして識別します。
no	すでにマウントされている FTP ファイル システムを削除し、アクセスできないようにします。
password *password*	ファイル システムのマウントのための認可されたパスワードを指定します。
path *pathname*	指定された FTP ファイル システム サーバへのディレクトリ パス名を指定します。パス名にスペースを含めることはできません。
server *server-name*	FTPFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
status enable/disable	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
username *username*	ファイル システムのマウントが認可されているユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
設定マウント ftp	•	•	•	—	•
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

mount *name* **type ftp** コマンドは、Installable File System（IFS）を使用して、指定されたネットワーク ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

FTP ファイル システムが実際にマウントされていることを確認するには、**dir all-filesystems** 命令を使用します。

mount コマンドに指定されているマウント名は、他の CLI コマンドがセキュリティ アプライアンスですでにマウントされているファイル システムを参照するときに使用されます。ローカル認証局用にファイル ストレージを設定する **database** コマンドでは、データベース ファイルをフラッシュ ストレージでないストレージに保存するために、すでにマウントされているファイル システムのマウント名が必要です。

（注） FTP-type マウントの作成時に **mount** コマンドを使用するには、FTP サーバに UNIX ディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています （**mount** *name* **type ftp** コマンドを参照）。Network File System（NFS; ネットワーク ファイル システム）ボリュームのマウントは、このリリースではサポートされていません。

例

次に、*ftp://amor;chief:big-kid@myfiler02* を *my ftp:* というラベルとしてマウントする例を示します。

```
hostname(config)# mount myftp type ftp server myfiler02a path status enable username
chief password big-kid
```

関連コマンド

コマンド	説明
debug webvpn	WebVPN デバッグ メッセージをロギングします。
ftp mode passive	セキュリティ アプライアンス上の FTP クライアントと FTP サーバとの通信を制御します。

mroute

スタティック マルチキャスト ルートを設定するには、グローバル コンフィギュレーション モードで **mroute** コマンドを使用します。スタティック マルチキャスト ルートを削除するには、このコマンドの **no** 形式を使用します。

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

構文の説明

dense *output_if_name*	（任意）デンス モード出力のインターフェイス名。 **dense** *output_if_name* キーワードと引数のペアは、SMR スタブ マルチキャスト ルーティング（igmp 転送）に対してだけサポートされます。
distance	（任意）ルートのアドミニストレーティブ ディスタンス。ディスタンスが小さいルートが優先されます。デフォルトは 0 です。
in_if_name	mroute の着信インターフェイス名を指定します。
rpf_addr	mroute の着信インターフェイスを指定します。RPF アドレスが PIM ネイバーである場合、PIM Join メッセージ、接合メッセージ、および Prune メッセージがそのアドレスに送信されます。*rpf-addr* 引数には、直接接続されたシステムのホスト IP アドレスまたはネットワーク / サブネット番号を指定します。ルートである場合、直接接続されたシステムを検索するために、ユニキャスト ルーティング テーブルから再帰検索が実施されます。
smask	マルチキャスト送信元ネットワーク アドレス マスクを指定します。
src	マルチキャスト送信元の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の検索場所をスタティックに設定できます。セキュリティ アプライアンスは、特定の送信元にユニキャスト パケットを送信する際に使用したものと同じインターフェイスでマルチキャスト パケットを受信するものと想定します。場合によっては、マルチキャスト ルーティングをサポートしないルートをバイパスするなど、マルチキャスト パケットがユニキャスト パケットとは別のパスをたどることがあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

マルチキャスト ルート テーブルの内容を表示するには、**show mroute** コマンドを使用します。実行コンフィギュレーションで mroute コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する例を示します。

```
hostname(config)# mroute 172.16.0.0 255.255.0.0 inside
```

関連コマンド

コマンド	説明
clear configure mroute	コンフィギュレーションから **mroute** コマンドを削除します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	コンフィギュレーションの **mroute** コマンドを表示します。

msie-proxy except-list

クライアント PC でローカル バイパスを対象に Microsoft Internet Explorer のブラウザ プロキシ例外リスト設定を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

構文の説明

none	IP アドレス / ホスト名またはポートがなく、例外リストを継承しないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、msie-proxy except-list はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次に、Microsoft Internet Explorer のプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy local-bypass

クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

構文の説明

disable	クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定をディセーブルにします。
enable	クライアント PC の Microsoft Internet Explorer のブラウザ プロキシ ローカル バイパス設定をイネーブルにします。

デフォルト

デフォルトでは、msie-proxy local-bypass はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer のプロキシ ローカル バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy method

クライアント PC のブラウザ プロキシ アクション（「メソッド」）を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

（注）　この構文に適用される条件については、「使用上のガイドライン」を参照してください。

構文の説明

auto-detect	クライアント PC の Internet Explorer または Firefox で自動プロキシ サーバ検出の使用をイネーブルにします。
no-modify	このクライアント PC では、ブラウザの HTTP ブラウザ プロキシ サーバ設定をそのままにしておきます。
no-proxy	このクライアント PC では、ブラウザの HTTP プロキシ設定をディセーブルにします。
use-pac-url	**msie-proxy pac-url** コマンドに指定されているプロキシ自動コンフィギュレーション ファイル URL から HTTP プロキシ サーバ設定を取得するように Internet Explorer に指示します。このオプションは、Internet Explorer にだけ有効です。
use-server	**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシ サーバ設定を設定します。

デフォルト

デフォルトのメソッドは use-server です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	use-pac-url オプションが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行には、最大 100 文字含めることができます。

Safari ブラウザは、auto-detect をサポートしません。Firefox ブラウザおよび Safari ブラウザでは、これらのコマンド オプションを一度に 1 つだけ使用できます。Microsoft Internet Explorer は、このコマンド オプションの次の組み合わせをサポートします。

[no] msie-proxy method no-proxy

[no] msie-proxy method no-modify

[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルは、Web サーバにあります。**use-pac-url** を指定すると、Internet Explorer は .pac ファイルを使用してプロキシ設定を判別します。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定として自動検出を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次に、クライアント PC のサーバとしてサーバ QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy pac-url	プロキシ自動コンフィギュレーション ファイルの取得先となる URL を指定します。
msie-proxy server	クライアント PC に対して、Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy pac-url

プロキシ情報の検索場所をブラウザに指示するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy pac-url** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

構文の説明

none	URL 値がないことを指定します。
value *url*	使用するプロキシ サーバが 1 つ以上定義されているプロキシ自動コンフィギュレーション ファイルをブラウザが取得できる Web サイトの URL を指定します。

デフォルト

デフォルト値は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

要件

プロキシ自動コンフィギュレーション機能を使用するには、リモート ユーザは Cisco AnyConnect VPN クライアントを使用する必要があります。プロキシ自動コンフィギュレーション URL の使用をイネーブルにするには、**msie-proxy method** コマンドを **use-pac-url** オプションとともに設定する必要があります。

このコマンドを使用する理由

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティングする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシ サーバを設定し、一時的な状態に基づいてユーザがその中からプロキシ サーバを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアント コンピュータに使用するかを決定する単一のスクリプト ファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシ サーバを指定します。
- ローカル サブネットを元に、ローミング ユーザ用に最も近いプロキシを指定します。

プロキシ自動コンフィギュレーション機能の使用方法

テキスト エディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバを指定するロジックを含む JavaScript ファイルです。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。次に、**msie-proxy method** コマンドに **use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。

例

次に、FirstGroup というグループ ポリシーのプロキシ設定を www.mycompanyserver.com という URL から取得するように、ブラウザを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url value http://www.mycompanyserver.com
hostname(config-group-policy)#
```

次に、FirstGroup というグループ ポリシーのプロキシ自動コンフィギュレーション機能をディセーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url none
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy method	クライアント PC のブラウザ プロキシ アクション（「メソッド」）を設定します。
msie-proxy server	クライアント PC に対して、Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy server

クライアント PC 用に Microsoft Internet Explorer のブラウザ プロキシ サーバおよびポートを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

構文の説明

none	プロキシ サーバに指定されている IP アドレス / ホスト名またはポートがなく、サーバが継承されないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号は任意です。

デフォルト

デフォルトでは、no msie-proxy server が指定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次に、Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

mtu

インターフェイスの最大伝送単位を指定するには、グローバル コンフィギュレーション モードで **mtu** コマンドを使用します。イーサネット インターフェイスの MTU ブロック サイズを 1500 にリセットするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。

mtu *interface_name bytes*

no mtu *interface_name bytes*

構文の説明

bytes	MTU のバイト数。有効な値は、64 ～ 65,535 バイトです。
interface_name	内部または外部ネットワーク インターフェイス名。

デフォルト

イーサネット インターフェイスのデフォルトの *bytes* は 1500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

mtu コマンドを使用すると、接続で送信されるデータ サイズを設定できます。MTU 値よりも大きいデータは、送信前にフラグメント化されます。

セキュリティ アプライアンスは、IP パス MTU ディスカバリを（RFC 1191 での規定に従って）サポートします。これにより、ホストはパスに沿ったさまざまなリンクで許容される最大 MTU サイズをダイナミックに検出し、各サイズの差に対処できます。パケットがインターフェイスに対して設定されている MTU よりも大きくなっているものの、「Don't Fragment」（DF）ビットが設定されているために、セキュリティ アプライアンスがデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、メッセージを送信ホストに送信して、問題を警告します。送信ホストは、パスに沿ったすべてのリンクのうち最小のパケット サイズに適合するように、宛先へのパケットをフラグメント化する必要があります。

イーサネット インターフェイスのブロックのデフォルトの MTU は 1500 バイトです（最大値でもあります）。ほとんどのアプリケーションではこの値で十分ですが、ネットワーク状況によってはこれよりも小さい値にすることもできます。

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を使用するときは、L2TP ヘッダーと IPSec ヘッダーの長さを踏まえて MTU サイズを 1380 に設定することを推奨します。

例

次に、インターフェイスの MTU を指定する例を示します。

```
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
hostname(config)# mtu inside 8192
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送単位値をクリアします。
show running-config mtu	現在の最大伝送単位のブロック サイズを表示します。

multicast boundary

管理用スコープのマルチキャスト アドレスのマルチキャスト境界を設定するには、インターフェイス コンフィギュレーション モードで **multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストには、境界の影響を受けるアドレスの範囲を定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL によって拒否された Auto-RP メッセージをフィルタリングします。指定されていない場合、すべての Auto-RP メッセージが通過します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、*acl* 引数によって定義されている範囲でマルチキャスト グループ アドレスをフィルタリングするようにインターフェイスに管理用スコープの境界を設定するために使用されます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。このコマンドが設定されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。マルチキャスト データ パケット フローを制限すると、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できます。

filter-autorp キーワードを設定した場合、管理用スコープの境界は Auto-RP 検出メッセージおよびアナウンス メッセージを調べ、境界 ACL によって拒否される Auto-RP パケットから Auto-RP グループ範囲アナウンスメントを削除します。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

例

次に、すべての管理用スコープのアドレスの境界を設定し、Auto-RP メッセージをフィルタリングする例を示します。

```
hostname(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
hostname(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# multicast boundary boundary_test filter-autorp
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

multicast-routing

セキュリティ アプライアンスの IP マルチキャスト ルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **multicast routing** コマンドを使用します。IP マルチキャスト ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

multicast-routing

no multicast-routing

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

multicast-routing コマンドは、デフォルトですべてのインターフェイスで PIM および IGMP をイネーブルにします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

multicast-routing コマンドは、すべてのインターフェイスで PIM および IGMP をイネーブルにします。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

セキュリティ アプライアンスが PIM RP である場合は、セキュリティ アプライアンスの未変換の外部アドレスを RP アドレスとして使用します。

マルチキャスト ルーティング テーブルのエントリの数は、システムに搭載されているメモリの量によって制限されます。表 20-3 に、セキュリティ アプライアンス上のメモリの量に基づく特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 20-3　マルチキャスト テーブルのエントリの制限

テーブル	16 MB	128 MB	128 + MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

例

次に、セキュリティ アプライアンスで IP マルチキャスト ルーティングをイネーブルにする例を示します。

```
hostname(config)# multicast-routing
```

関連コマンド

コマンド	説明
igmp	インターフェイスに対して IGMP をイネーブルにします。
pim	インターフェイス上の PIM をイネーブルにします。

CHAPTER 21

nac policy コマンド～ override-svc-download コマンド

nac-policy

シスコ Network Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを作成またはアクセスし、そのタイプを指定するには、グローバル コンフィギュレーション モードで **nac-policy** コマンドを使用します。NAC ポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

```
nac-policy nac-policy-name nac-framework

[no] nac-policy nac-policy-name nac-framework
```

構文の説明

nac-policy-name	NAC ポリシーの名前。最大 64 文字で NAC ポリシーの名前を指定します。**show running-config nac-policy** コマンドは、セキュリティ アプライアンスにすでに存在する各 NAC ポリシーの名前およびコンフィギュレーションを表示します。
nac-framework	NAC フレームワークを使用して、リモート ホストのネットワーク アクセス ポリシーを提供することを指定します。セキュリティ アプライアンスの NAC フレームワーク サービスを提供するには、シスコ アクセス コントロール サーバがネットワークに存在している必要があります。 このタイプを指定した場合、プロンプトは現在のモードが設定 nac ポリシー nac フレームワーク コンフィギュレーション モードであることを示します。このモードでは、NAC フレームワーク ポリシーを設定できます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

グループ ポリシーに割り当てられる NAC アプライアンスごとにこのコマンドを一度使用します。次に、**nac-settings** コマンドを使用して、該当する各グループ ポリシーに NAC ポリシーを割り当てます。IPSec または Cisco AnyConnect VPN トンネルのセットアップ時に、セキュリティ アプライアンスは使用中のグループ ポリシーに関連付けられた NAC ポリシーを適用します。

NAC ポリシーが 1 つ以上のグループ ポリシーにすでに割り当てられている場合、**no nac-policy** *name* コマンドではその NAC ポリシーを削除できません。

例

次のコマンドでは、NAC フレームワーク ポリシーを nac-framework1 という名前で作成し、そのポリシーにアクセスしています。

```
hostname(config)# nac-policy nac-framework1 nac-framework
hostname(config-nac-policy-nac-framework)
```

次のコマンドでは、nac-framework1 という名前の NAC フレームワーク ポリシーを削除しています。

```
hostname(config)# no nac-policy nac-framework1
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
show running-config nac-policy	セキュリティ アプライアンス上の各 NAC ポリシーのコンフィギュレーションを表示します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
clear configure nac-policy	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーを実行コンフィギュレーションから削除します。

nac-settings

NAC ポリシーをグループ ポリシーに割り当てるには、次のようにグループ ポリシー コンフィギュレーション モードで **nac-settings** コマンドを使用します。

nac-settings {**value** *nac-policy-name* | **none**}

[**no**] **nac-settings** {**value** *nac-policy-name* | **none**}

構文の説明

nac-policy-name	グループ ポリシーに割り当てられる NAC ポリシー。名前を付ける NAC ポリシーは、セキュリティ アプライアンスのコンフィギュレーションに存在している必要があります。**show running-config nac-policy** コマンドは、各 NAC ポリシーの名前および設定を表示します。
none	グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。
value	名前を付ける NAC ポリシーをグループ ポリシーに割り当てます。

デフォルト

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

nac-policy コマンドを使用して NAC ポリシーの名前およびタイプを指定してから、このコマンドを使用してそれをグループ ポリシーに割り当てます。

show running-config nac-policy コマンドは、各 NAC ポリシーの名前および設定を表示します。

NAC ポリシーをグループ ポリシーに割り当てると、セキュリティ アプライアンスはそのグループ ポリシーの NAC を自動的にイネーブルにします。

例

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除しています。グループ ポリシーは、デフォルトのグループ ポリシーから *nac-settings* 値を継承します。

```
hostname(config-group-policy)# no nac-settings
hostname(config-group-policy)
```

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにしています。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。

```
hostname(config-group-policy)# nac-settings none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
show running-config nac-policy	セキュリティ アプライアンス上の各 NAC ポリシーのコンフィギュレーションを表示します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

name

IP アドレスに名前を関連付けるには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。テキスト名の使用はディセーブルにするが、コンフィギュレーションからは削除しない場合は、このコマンドの **no** 形式を使用します。

name *ip_address name* [description *text*]]

no name *ip_address* **[***name* [description *text*]**]**

構文の説明

description	（任意）IP アドレス名の説明を指定します。
ip_address	名前を付けるホストの IP アドレスを指定します。
name	IP アドレスに割り当てられる名前を指定します。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアです。*name* は、63 文字以下である必要があります。また、*name* は数値で開始できません。
text	説明のテキストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.0(4)	このコマンドは、任意の説明を含めることができるように拡張されました。

使用上のガイドライン

名前と IP アドレスとの関連付けをイネーブルにするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に **names** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドを使用した直後、かつ **write memory** コマンドよりも前に使用します。

name コマンドを使用すると、テキスト名でホストを識別し、テキスト ストリングを IP アドレスにマッピングします。**no name** コマンドを使用すると、テキスト名の使用をディセーブルにできます。ただし、コンフィギュレーションからはテキスト名は削除されません。コンフィギュレーションから名前のリストをクリアするには、**clear configure name** コマンドを使用します。

name 値の表示をディセーブルにするには、**no names** コマンドを使用します。

name コマンドと **names** コマンドは両方ともコンフィギュレーションに保存されます。

name コマンドは、ネットワーク マスクへの名前の割り当てをサポートしません。たとえば、次のコマンドは拒否されます。

```
hostname(config)# name 255.255.255.0 class-C-mask
```

（注） マスクを必要とするいずれのコマンドも、受け入れ可能なネットワーク マスクとして名前を処理できません。

例

次に、**names** コマンドを使用して、**name** コマンドの使用をイネーブルにする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示をディセーブルにします。後で **names** コマンドを使用すると、**name** コマンド値が再度表示されるようになります。

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

hostname(config)# no names
hostname(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

hostname(config)# names
hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
names	名前と IP アドレスの関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスの名前を指定するには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。インターフェイス名はインターフェイス タイプおよび ID（gigabitethernet0/1 など）ではなくセキュリティ アプライアンスのすべてのコンフィギュレーション コマンドで使用されるため、インターフェイス名がないとトラフィックはインターフェイスを通過できません。

nameif *name*

no nameif

構文の説明

name	最大 48 文字で名前を設定します。名前は大文字と小文字が区別されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、**nameif** コマンドを入力する前に、**vlan** コマンドで VLAN を割り当てる必要があります。

名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

例

次に、2 つのインターフェイスにそれぞれ「inside」と「outside」という名前を設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/0
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
```

```
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

名前と IP アドレスの関連付けをイネーブルにするには、グローバル コンフィギュレーション モードで **names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。**name** 値の表示をディセーブルにするには、**no names** コマンドを使用します。

names

no names

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

names コマンドは、**name** コマンドで設定した名前と IP アドレスの関連付けをイネーブルにするために使用します。**name** または **names** コマンドを入力する順序は、重要ではありません。

例

次に、名前と IP アドレスの関連付けをイネーブルにする例を示します。

```
hostname(config)# names
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられた名前のリストを表示します。
show running-config names	IP アドレスと名前の変換を表示します。

name-separator

電子メール、VPN ユーザ名、パスワード間のデリミタとなる文字を指定するには、適用可能な電子メール プロキシ モードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** 形式を使用します。

name-separator [*symbol*]

no name-separator

構文の説明

symbol	（任意）電子メール、VPN ユーザ名、パスワードを区切る文字。選択肢は「@」（アット マーク）、「|」（パイプ）、「:（コロン）」、「|（ハッシュ）」、「,（カンマ）」、「;」（セミコロン）です。

デフォルト

デフォルトは「:」（コロン）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前の区切り文字には、サーバの区切り文字とは異なる文字を使用する必要があります。

例

次に、番号記号（#）を POP3S の名前区切り文字として設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバ名を区切ります。

name-server

1 つ以上の DNS サーバを識別するには、DNS サーバ グループ コンフィギュレーション モードで **name-server** コマンドを使用します。1 つ以上のサーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、DNS を使用して、SSL VPN コンフィギュレーションまたは証明書設定のサーバ名を解決します（サポートされているコマンドのリストについては、「使用上のガイドライン」を参照してください）。サーバ名（AAA など）を定義するその他の機能は、DNS 解決をサポートしていません。IP アドレスを入力するか、または **name** コマンドを使用して名前を IP アドレスに手動で解決する必要があります。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

構文の説明

ip_address	DNS サーバの IP アドレスを指定します。最大 6 つのアドレスを個別のコマンドとして指定するか、便宜上最大 6 つのアドレスをスペースで区切って 1 つのコマンドで指定できます。1 つのコマンドに複数のサーバを入力した場合、セキュリティ アプライアンスはそれぞれのサーバを個別のコマンドとしてコンフィギュレーションに保存します。セキュリティ アプライアンスでは、応答を受信するまで各 DNS サーバを順に試します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DNS サーバ グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ルックアップをイネーブルにするには、DNS サーバ グループ コンフィギュレーション モードで **domain-name** コマンドを設定します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

DNS 解決をサポートする SSL VPN コマンドには、次のものがあります。

- **server（pop3s）**
- **server（imap4s）**
- **server（smtps）**
- **port-forward**

- **url-list**

DNS 解決をサポートする証明書のコマンドには、次のものがあります。

- **enrollment url**
- **url**

name コマンドを使用して、名前および IP アドレスを手動で入力できます。

例

次に、3 つの DNS サーバをグループ「dnsgroup1」に追加する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

セキュリティ アプライアンスは、次のように、別々のコマンドとしてコンフィギュレーションを保存します。

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

さらに 2 つのサーバを追加するには、それらを 1 つのコマンドとして入力します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

DNS サーバ グループ コンフィギュレーションを確認するには、グローバル コンフィギュレーション モードで **show running-config dns** コマンドを入力します。

```
hostname(config)# show running-config dns
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
name-server 10.5.1.1
name-server 10.8.3.8
...
```

また、それらを 2 つの個別のコマンドとして入力することもできます。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1
hostname(config)# name-server 10.8.3.8
```

複数のサーバを削除するには、次のようにそれらのサーバを複数のコマンドまたは 1 つのコマンドとして入力します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

nat

あるインターフェイス上のアドレスのうち、別のインターフェイス上のマッピング先のアドレスに変換されるアドレスを識別するには、グローバル コンフィギュレーション モードで **nat** コマンドを使用します。このコマンドは、プールされたマッピング先のアドレスのいずれかにアドレスが変換されるダイナミック NAT または PAT を設定します。**nat** コマンドを削除するには、このコマンドの **no** 形式を使用します。

通常のダイナミック NAT の場合：

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

ポリシー ダイナミック NAT および NAT 免除の場合：

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

構文の説明

access-list *access_list_name*	ポリシー NAT とも呼ばれる拡張アクセス リストを使用して、ローカル アドレスおよび宛先アドレスを識別します。**access-list** コマンドを使用して、アクセス リストを作成します。**eq** 演算子を使用して、アクセス リストに任意でローカル ポートおよび宛先ポートを指定できます。NAT ID が **0** の場合、アクセス リストでは NAT が免除されるアドレスが指定されます。NAT 免除は、ポリシー NAT と同じではありません。NAT 免除では、たとえば、ポート アドレスは指定できません。 **（注）** **show access-list** コマンドによって表示されるアクセス リストのヒット カウントは、NAT 免除アクセス リストでは増加しません。
dns	（任意）このコマンドに一致する DNS 応答で A レコード（アドレス レコード）を書き換えます。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。 DNS サーバにエントリがあるホストのアドレスが NAT ステートメントに含まれ、その DNS サーバがクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストにそれぞれ異なるアドレスを必要とします。つまり、一方はグローバル アドレスを必要とし、もう一方はローカル アドレスを必要とします。変換されたホストは、クライアントまたは DNS サーバと同じインターフェイスに存在する必要があります。一般に、他のインターフェイスからのアクセスを許可する必要があるホストは static 変換を使用するため、**static** コマンドではこのオプションの方が使用される可能性が高くなります。

emb_limit	（任意）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。
mask	（任意）実アドレスのサブネット マスクを指定します。マスクを入力しないと、IP アドレス クラスのデフォルト マスクが使用されます。
nat_id	NAT ID の整数を指定します。通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（nat id access-list）の場合、整数の範囲は 1 ～ 65535 となります。 アイデンティティ NAT（**nat 0**）および NAT 免除（**nat 0 access-list**）は、NAT ID に **0** を使用します。 この ID は、グローバル プールを *real_ip* に関連付けるために、**global** コマンドで参照されます。
norandomseq	（任意）TCP ISN のランダム化保護をディセーブルにします。NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。 それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。 保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。 TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。 • 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。 • セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
outside	（任意）このインターフェイスが **global** ステートメントの照合によって識別したインターフェイスよりも低いセキュリティ レベルにある場合、**outside** を入力する必要があります。この機能は、外部 NAT または双方向 NAT と呼ばれます。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実アドレスを指定します。**0.0.0.0**（または短縮形 **0**）を使用して、すべてのアドレスを指定できます。

tcp *tcp_max_conns*	（任意）ローカル ホストに許可する同時 TCP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します （アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。
udp *udp_max_conns*	（任意）ローカル ホストに許可する同時 UDP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します （アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。 NAT 免除（**nat 0 access-list**）はサポートされていません。この引数は CLI で入力できますが、コンフィギュレーションには保存されません。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、1 つの **global** コマンドと一致します。

NAT コントロール

セキュリティ アプライアンスは、NAT ルールがトラフィックに一致すると、アドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。例外は、**nat-control** コマンドを使用して NAT コントロールをイネーブルにした場合です。NAT コントロールをイネーブルにした場合、セキュリティの高いインターフェイス（inside）からセキュリティの低いインターフェイス（outside）に移動するパケットは NAT ルールに一致する必要があり、一致しないとそのパケットの処理は停止します。セキュリティ レベルが同じインターフェイス間では、NAT コントロールをイネーブルにした場合でも、NAT は必要ありません。必要に応じて任意で NAT を設定できます。**nat-control** コマンドは、旧バージョンのセキュリティ アプライアンスで定義された NAT コンフィギュレーションに対して使用します。NAT ルールが存在しないことに基づくのではなく、アクセス コントロールにアクセス ルールを使用して、セキュリティ アプライアンスを通過するトラフィックを阻止することがベスト プラクティスです。

ダイナミック NAT の概要

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピング プールには、実アドレス グループよりも少ない数のアドレスを含めることができます。変換対象のホストが宛先ネットワークにアクセスすると、セキュリティ アプライアンスは、マッピング プールから IP アドレスをそのホストに割り当てます。この変換は、実ホストが接続を開始するときにだけ追加されます。変換は、接続が維持されている間のみ機能します。変換がタイムアウトすると、ユーザが同じ IP アドレスを保持することはありません（**timeout xlate** コマンドを参照）。このため、宛先ネットワーク上のユーザはダイナミック NAT（または PAT）を使用するホストへの接続を（接続がアクセス リストで許容されていても）確実には開始できません。セキュリティ アプライアンスは、実ホスト アドレスへの直接接続を拒否します。ホストへの信頼性の高いアクセスについては、**static** コマンドを参照してください。

ダイナミック NAT の長所と短所

ダイナミック NAT には、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  この事象が発生した場合には、PAT を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールでは、ルーティング可能なアドレスを多数使用する必要があります。インターネットのように宛先ネットワークで登録済みアドレスが必要になる場合は、使用可能なアドレスが不足することがあります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は GRE バージョン 0 などポートが過負荷にならない IP プロトコルでは機能しません。また、データ ストリームと制御パスが別々のポートにあり、オープン規格でないアプリケーション（一部のマルチメディア アプリケーション）でも機能しません。

ダイナミック PAT の概要

PAT は、複数の実アドレスを単一のマッピング IP アドレスに変換します。特に、セキュリティ アプライアンスは実アドレスと送信元ポート（実ソケット）をマッピング先のアドレスと 1024 より上の一意のポート（マッピング ソケット）に変換します。接続ごとに送信元ポートが異なるため、それぞれの接続で個別に変換を行う必要があります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れると、ポート変換も 30 秒間の非アクティブ状態の後に有効期限切れになります。このタイムアウトは変更できません。

PAT では単一のマッピング先のアドレスを使用するため、ルーティング可能なアドレスの使用を抑えることができます。さらに、セキュリティ アプライアンス インターフェイスの IP アドレスを PAT アドレスとして使用できます。PAT は、データ ストリームが制御パスとは別のものであるマルチメディア アプリケーションでは機能しません。

（注）　変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。アドレス（実アドレスとマッピング先のアドレスの両方）は予測できないため、ホストへの接続が確立される可能性はほとんどありません。ただし、この場合、アクセス リストのセキュリティを利用できます。

NAT のバイパス

NAT コントロールをイネーブルにした場合、内部ホストは、外部ホストにアクセスするときに NAT ルールに一致する必要があります。一部のホストに対して NAT を実行しない場合は、それらのホストに関する NAT をバイパスします（あるいは、NAT コントロールをディセーブルにします）。NAT をサポートしないアプリケーションを使用している場合などには、NAT をバイパスすることを推奨します。**static** コマンドを使用すると、NAT や次のいずれかのオプションをバイパスできます。

- アイデンティティ NAT（**nat 0** コマンド）：アイデンティティ NAT（ダイナミック NAT に似ています）を設定するときは、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続にアイデンティティ NAT を使用する必要があります。このため、インターフェイス A にアクセスするときには実アドレスに対して通常の変換の実行を選択できませんが、インターフェイス B にアクセスするときにはアイデンティティ NAT を使用できます。一方、通常のダイナミック NAT では、アドレス変換を実施する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実アドレスが、アクセス リストに従って使用できるすべてのネットワークでルーティング可能であることを確認します。

  アイデンティティ NAT の場合、マッピング先のアドレスは実アドレスと同じですが、外部から内部への接続を（インターフェイスのアクセス リストで許可されていても）開始できません。この機能には、スタティックなアイデンティティ NAT または NAT 免除を使用してください。

- NAT 免除（**nat 0 access-list** コマンド）：NAT 免除を使用すると、変換後のホストとリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実アドレスを判別するときに実アドレスおよび宛先アドレスを指定できるため（ポリシー NAT に似ています）、NAT 免除を使用する方が制御の柔軟性が増します。その反面、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートが考慮されません。また、NAT 免除は **tcp** キーワードや **udp** キーワードなどの接続設定をサポートしません。

ポリシー NAT

ポリシー NAT を使用すると、拡張アクセス リストに送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換の実アドレスを識別できます。任意で送信元ポートおよび宛先ポートを指定することもできます。通常の NAT でのみ、実アドレスを考慮できます。たとえば、実アドレスがサーバ A にアクセスするときにはその実アドレスをマッピング先のアドレス A に変換できますが、実アドレスがサーバ B にアクセスするときにはその実アドレスをマッピング先のアドレス B に変換できます。

セカンダリ チャネルのアプリケーション インスペクションを必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

（注）　NAT 免除以外のすべてのタイプの NAT が、ポリシー NAT をサポートします。NAT 免除はアクセス リストを使用して実アドレスを識別しますが、ポリシー NAT とは異なり、ポートが考慮されません。ポリシー NAT をサポートする**スタティックな**アイデンティティ NAT を使用すると、NAT 免除と同じ結果を得ることができます。

モジュラ ポリシー フレームワーク を使用した接続設定

モジュラ ポリシー フレームワーク を使用することによっても、接続制限を設定できます（ただし、初期接続制限は設定できません）。詳細については、**set connection** コマンドを参照してください。初期接続制限を設定するには、NAT を使用する必要があります。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
```

```
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
clear configure nat	NAT コンフィギュレーションを削除します。
global	グローバル アドレスのプールからエントリを作成します。
interface	インターフェイスを作成および設定します。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

nat（vpn ロードバランシング）

このデバイスの IP アドレスを NAT でどの IP アドレスに変換するかを設定するには、VPN ロード バランシング コンフィギュレーション モードで **nat** コマンドを使用します。この NAT 変換をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat *ip-address*

no nat [*ip-adddress*]

構文の説明

ip-address	この NAT でこのデバイスの IP アドレスの変換先となる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始する必要があります。

このコマンドの **no nat** 形式で任意の *ip-address* 値を指定する場合は、IP アドレスが実行コンフィギュレーションの既存の NAT IP アドレスに一致する必要があります。

例

次に、nat コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。この **nat** コマンドでは、NAT で変換するアドレスを 192.168.10.10 に設定しています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
```

```
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

nat-control

NAT コントロールを有効にするには、グローバル コンフィギュレーション モードで **nat-control** コマンドを使用します。内部ホストが外部にアクセスする場合は、NAT コントロールに内部ホストの NAT が必要になります。NAT コントロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-control

no nat-control

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

NAT コントロールは、デフォルトではディセーブルです（**no nat-control** コマンド）。ただし、旧バージョンのソフトウェアからアップグレードした場合には、システムで NAT コントロールがイネーブルになっていることがあります。旧バージョンによってはイネーブルがデフォルトであったためです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.3.(1)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

NAT コントロールをイネーブルにした場合、内部インターフェイスから外部インターフェイスに移動するパケットは NAT ルールに一致する必要があります。内部ネットワーク上のホストが外部ネットワーク上のホストにアクセスする場合には、内部ホストのアドレスを変換するように NAT を設定する必要があります。

nat-control コマンドは、旧バージョンのセキュリティ アプライアンスで定義された NAT コンフィギュレーションに対して使用します。NAT ルールが存在しないことに基づくのではなく、アクセス コントロールにアクセス ルールを使用して、セキュリティ アプライアンスを通過するトラフィックを阻止することがベスト プラクティスです。

セキュリティ レベルが同じインターフェイス同士で通信する場合には、NAT を使用する必要はありません。ただし、NAT コントロールをイネーブルにして同じセキュリティのインターフェイスにダイナミック NAT または PAT を設定した場合は、インターフェイスから同じセキュリティのインターフェイスまたは外部インターフェイスに移動するすべてのトラフィックが、NAT ルールに一致する必要があります。

同様に、NAT コントロールで外部ダイナミック NAT または PAT をイネーブルにした場合は、内部インターフェイスにアクセスするときには、すべての外部トラフィックが NAT ルールに一致する必要があります。

NAT コントロールをイネーブルにしたスタティック NAT では、これらの制限がありません。

デフォルトでは、NAT コントロールはディセーブルであるため、NAT の実行を選択しない限り、どのネットワークでも NAT を実行する必要はありません。

（注） マルチ コンテキスト モードでは、パケット分類子が NAT コンフィギュレーションを利用してパケットをコンテキストに割り当てる場合があります。NAT コントロールがディセーブルであるために NAT を実行しない場合は、ネットワーク設定の変更が必要になることがあります。

NAT コントロールのセキュリティは強化するものの、場合によっては内部アドレスを変換しないようにする場合は、その内部アドレスに NAT 免除（**nat 0 access-list**）またはアイデンティティ NAT（**nat 0** または **static**）ルールを適用できます。

no-nat control コマンドで NAT コントロールがディセーブルにされており、インターフェイスに NAT と global コマンドのペアが設定されている場合、実 IP アドレスから他のインターフェイスに移動するには、**nat 0 access-list** コマンドでその宛先を定義する必要があります。

たとえば、次の NAT は外部ネットワークに移動するときに実施したものです。

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
```

上記のコンフィギュレーションでは、内部ネットワークであらゆるデータを捕捉するため、内部アドレスが DMZ に移動するときにその内部アドレスを変換しない場合は、次の例に示すように、NAT 免除に関してトラフィックを照合する必要があります。

```
access-list EXEMPT extended permit ip any 192.168.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
access-list EXEMPT extended permit ip any 10.1.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ2
nat (inside) 0 access-list EXEMPT
```

この他に、すべてのインターフェイスで NAT 変換を実行することもできます。

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
global (dmz1) 1 192.168.1.230
global (dmz2) 1 10.1.1.230
```

例

次に、NAT コントロールをイネーブルにする例を示します。

```
hostname(config)# nat-control
```

関連コマンド

コマンド	説明
nat	インターフェイス上で、別のインターフェイス上のマッピング先のアドレスに変換されるアドレスを定義します。
show running-config nat-control	NAT コンフィギュレーション要件を表示します。
static	実アドレスをマッピング先のアドレスに変換します。

nat-rewrite

DNS 応答の A レコードに組み込まれている IP アドレスの NAT リライトをイネーブルにするには、パラメータ コンフィギュレーション モードで **nat-rewrite** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-rewrite

no nat-rewrite

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

NAT リライトは、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションに **no nat-rewrite** を明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この機能は、DNS 応答の A タイプの Resource Record（RR; リソース レコード）の NAT 変換を実行します。

例

次に、DNS インスペクション ポリシー マップで NAT リライトをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# nat-rewrite
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

nbns-server（トンネル グループ webvpn 属性モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。コンフィギュレーションから NBNS サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバに照会します。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

構文の説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	これは WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバへのクエリーを再試行する回数を指定します。セキュリティ アプライアンスは、エラー メッセージを送信するまでに、ここに指定する回数、サーバのリストを循環して使用します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	NBNS サーバが 1 つだけ存在する場合は同じサーバに、複数存在する場合は別のサーバに、セキュリティ アプライアンスがクエリーを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。

デフォルト

NBNS サーバは、デフォルトでは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

サーバ エントリは最大 3 つです。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。

no オプションを使用して、コンフィギュレーションから一致するエントリを削除します。

例

次に、NBNS サーバでトンネル グループ「test」を設定する例を示します。NBNS サーバはマスター ブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバを設定する例も示します。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	指定したトンネル グループの WebVPN 属性を指定します。

nbns-server（webvpn モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。コンフィギュレーションから NBNS サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、NetBIOS 名を IP アドレスにマップするために NBNS サーバに照会します。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

構文の説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	これは WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバへのクエリーを再試行する回数を指定します。セキュリティ アプライアンスは、エラー メッセージを送信するまでに、ここに指定する回数、サーバのリストを循環して使用します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	NBNS サーバが 1 つだけ存在する場合は同じサーバに、複数存在する場合は別のサーバに、セキュリティ アプライアンスがクエリーを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。

デフォルト

NBNS サーバは、デフォルトでは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

このコマンドは、webvpn コンフィギュレーション モードでは廃止されました。トンネル グループ webvpn 属性コンフィギュレーション モードの nbns-server コマンドに置き換えられました。リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性モードの同等のコマンドに変換されます。

サーバ エントリは最大 3 つです。冗長性のために、設定する最初のサーバはプライマリ サーバで、その他のサーバはバックアップです。

no オプションを使用して、コンフィギュレーションから一致するエントリを削除します。

例

次に、NBNS サーバを設定する例を示します。NBNS サーバはマスター ブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバを設定する例も示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

ポイントツーポイントの非ブロードキャスト ネットワークにスタティック ネイバーを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。コンフィギュレーションからスタティックに定義されたネイバーを削除するには、このコマンドの **no** 形式を使用します。**neighbor** コマンドは、VPN トンネル経由で OSPF ルートをアドバタイズするために使用されます。

neighbor *ip_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

構文の説明

interface *name*	（任意）**nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	隣接ルータの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

既知の非ブロードキャスト ネットワーク ネイバーごとにネイバー エントリを 1 つ含める必要があります。ネイバー アドレスは、インターフェイスのプライマリ アドレスに存在する必要があります。

ネイバーがシステムに直接接続されたいずれかのインターフェイスと同じネットワークにないときには、**interface** オプションを指定する必要があります。また、ネイバーに到達するには、スタティック ルートを作成する必要があります。

例

次に、アドレス 192.168.1.1 で隣接ルータを定義する例を示します。

```
hostname(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

neighbor（EIGRP）

ルーティング情報を交換する EIGRP 隣接ルータを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。ネイバー エントリを削除するには、このコマンドの **no** 形式を使用します。

neighbor *ip_address* **interface** *name*

no neighbor *ip_address* **interface** *name*

構文の説明

interface *name*	**nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	隣接ルータの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

複数のネイバー ステートメントを使用して、特定の EIGRP ネイバーでピアリング セッションを確立できます。EIGRP がルーティング更新を交換するインターフェイスは、ネイバー ステートメントで指定する必要があります。2 つの EIGRP ネイバーがルーティング更新を交換するインターフェイスは、同じネットワークにある IP アドレスで設定する必要があります。

（注）　インターフェイスに対して **passive-interface** コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング更新および hello メッセージが表示されなくなります。EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

EIGRP hello メッセージは、**neighbor** コマンドを使用して定義されたネイバーにユニキャスト メッセージとして送信されます。

例

次に、ネイバーを 192.168.1.1 および 192.168.2.2 として EIGRP ピアリング セッションを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.0.0
```

```
hostname(config-router)# neighbor 192.168.1.1 interface outside
hostname(config-router)# neighbor 192.168.2.2 interface branch_office
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバー メッセージに関するデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

nem

ハードウェア クライアントのネットワーク拡張モードをイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。NEM をディセーブルにするには、**nem disable** コマンドを使用します。実行コンフィギュレーションから NEM 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

nem {**enable** | **disable**}

no nem

構文の説明

disable	ネットワーク拡張モードをディセーブルにします。
enable	ネットワーク拡張モードをイネーブルにします。

デフォルト

ネットワーク拡張モードはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

使用上のガイドライン

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークへの単一のルーティング可能なネットワークを提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

network

RIP ルーティング プロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr*

no network *ip_addr*

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、RIP ルーティング プロセスに参加します。

デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

指定されたネットワーク番号は、サブネット情報に含めないでください。ルータで使用できる network コマンドの数に制限はありません。指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング更新が送受信されます。また、インターフェイスのネットワークが指定されていない場合は、どの RIP ルーティング更新でもインターフェイスがアドバタイズされません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして RIP を定義する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# network 192.168.7.0
```

関連コマンド

コマンド	説明
router rip	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

network（EIGRP）

EIGRP ルーティング プロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr* [*mask*]

no network *ip_addr* [*mask*]

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、EIGRP ルーティング プロセスに参加します。
mask	（任意）IP アドレスのネットワーク マスク。

デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

network コマンドは、指定されたネットワークに IP アドレスが少なくとも 1 つ存在するすべてのインターフェイスで EIGRP を開始します。また、指定されたネットワークから接続済みのサブネットを EIGRP トポロジ テーブルに挿入します。

次に、セキュリティ アプライアンスは一致したインターフェイス経由でネイバーを確立します。セキュリティ アプライアンスに設定できる **network** コマンドの数に制限はありません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして EIGRP を定義する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 255.0.0.0
hostname(config-router)# network 192.168.7.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp interfaces	EIGRP に設定されているインターフェイスに関する情報を表示します。
show eigrp topology	EIGRP トポロジ テーブルを表示します。

network-acl

access-list コマンドを使用して以前に設定したファイアウォールの ACL 名を指定するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **network-acl** コマンドを使用します。既存のネットワーク ACL を削除するには、このコマンドの **no** 形式を使用します。すべてのネットワーク ACL を削除するには、このコマンドを引数なしで使用します。

network-acl *name*

no network-acl [*name*]

構文の説明

name	ネットワーク ACL の名前を指定します。最大 240 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

複数のファイアウォール ACL を DAP レコードに割り当てるには、このコマンドを複数回使用します。

セキュリティ アプライアンスは、指定された各 ACL を検証して、アクセス リスト エントリの許可ルールのみまたは拒否ルールのみが含まれていることを確認します。指定されたいずれかの ACL に許可ルールと拒否ルールが混在していた場合、セキュリティ アプライアンスはコマンドを拒否します。

次に、Finance Restrictions というネットワーク ACL を Finance という DAP レコードに適用する例を示します。

```
hostname(config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# network-acl Finance Restrictions
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
access-policy	ファイアウォール アクセス ポリシーを設定します。

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

network area

OSPF が動作するインターフェイスを定義し、そのインターフェイスのエリア ID を定義するには、ルータ コンフィギュレーション モードで **network area** コマンドを使用します。アドレス/ネットマスクのペアで定義されたインターフェイスの OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

network *addr mask* **area** *area_id*

no network *addr mask* **area** *area_id*

構文の説明

addr	[IP Address]。
area *area_id*	OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進表記で指定できます。10 進表記で指定する場合、有効な値の範囲は、0 ～ 4294967295 です。
mask	ネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

インターフェイスで OSPF を動作させるには、インターフェイスのアドレスを **network area** コマンドの対象にする必要があります。**network area** コマンドがインターフェイスの IP アドレスを対象にしていない場合、そのインターフェイスを経由する OSPF はイネーブルになりません。

セキュリティ アプライアンスで使用できる **network area** コマンドの数に制限はありません。

例

次に、192.168.1.1 インターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てる例を示します。

```
hostname(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

network-object

ネットワーク オブジェクトをネットワーク オブジェクト グループに追加するには、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用します。ネットワーク オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object host *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

構文の説明

host_addr	ホスト IP アドレス（ホスト名が **name** コマンドを使用してすでに定義されていない場合）。
host_name	ホスト名（ホスト名が **name** コマンドを使用して定義されている場合）。
net_addr	ネットワーク アドレス。サブネット オブジェクトを定義するために *netmask* とともに使用します。
netmask	ネットマスク。サブネット オブジェクトを定義するために *net_addr* とともに使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ネットワーク コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

network-object コマンドは、ネットワーク コンフィギュレーション モードでホストまたはサブネット オブジェクトを定義するために、**object-group** コマンドとともに使用します。

例

次に、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用して、新規にネットワーク オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
```

```
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

nt-auth-domain-controller

このサーバの NT プライマリ ドメイン コントローラの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **nt-auth-domain-controller** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

nt-auth-domain-controller *string*

no nt-auth-domain-controller

構文の説明

string	このサーバのプライマリ ドメイン コントローラの名前を最大 16 文字で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT 認証 AAA サーバに対してのみ有効です。ホスト コンフィギュレーション モードを開始するには、**aaa-server host** コマンドを先に使用する必要があります。*string* 変数の名前は、そのサーバ自体の NT エントリに一致する必要があります。

例

次に、このサーバの NT プライマリ ドメイン コントローラの名前を「primary1」に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。

clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

ntp authenticate

NTP サーバによる認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ntp authenticate** コマンドを使用します。NTP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ntp authenticate

no ntp authenticate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

認証をイネーブルにした場合、NTP サーバがパケットで正しい信頼できるキーを使用しているのであれば（**ntp trusted-key** コマンドを参照）、セキュリティ アプライアンスはその NTP サーバとのみ通信します。また、セキュリティ アプライアンスは認証キーを使用して NTP サーバと同期します（**ntp authentication-key** コマンドを参照）。

例

次に、NTP パケットで認証キー 42 を提供するシステムにのみ同期するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。

コマンド	説明
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバで認証するキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

ntp authentication-key *key_id* **md5** *key*

no ntp authentication-key *key_id* [**md5** *key*]

構文の説明

key_id	キー ID 1 ～ 4294967295 を識別します。この ID は、**ntp trusted-key** コマンドを使用して信頼できるキーとして指定する必要があります。
md5	認証アルゴリズムを MD5 として指定します。サポートされている唯一のアルゴリズムが MD5 です。
key	キー値を最大 32 文字のストリングとして設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 および 2 を指定して、信頼できる各キーの認証キーを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

NTP サーバを指定して、セキュリティ アプライアンス上の時間を設定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。複数のサーバを識別できます。セキュリティ アプライアンス では、最も正確なサーバを使用します。マルチ コンテキスト モードでは、システム コンフィギュレーションにのみ NTP サーバを設定します。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

構文の説明

ip_address	NTP サーバの IP アドレスを設定します。
key *key_id*	**ntp authenticate** コマンドを使用して認証をイネーブルにした場合は、このサーバの信頼できるキー ID を設定します。**ntp trusted-key** コマンドも参照してください。
source *interface_name*	ルーティング テーブルにデフォルトのインターフェイスを使用しない場合に、NTP パケットの発信インターフェイスを識別します。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。
prefer	精度に差がないサーバが複数ある場合は、この NTP サーバを優先サーバとして設定します。NTP では、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。サーバの精度に差がない場合は、**prefer** キーワードにどのサーバを使用するかを指定します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、セキュリティ アプライアンス では、精度の高いそのサーバを使用します。たとえば、セキュリティ アプライアンスは優先サーバであるストラタム 3 サーバよりもストラタム 2 のサーバを優先的に使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、送信元インターフェイスを任意とするように変更されました。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

NTP サーバによる認証を必要とする信頼できるキーに認証キー ID を指定するには、グローバル コンフィギュレーション モードで **ntp trusted-key** コマンドを使用します。信頼できるキーを削除するには、このコマンドの **no** 形式を使用します。複数のサーバで使用できるように複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

構文の説明

key_id	キー ID 1 ～ 4294967295 を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。サーバと同期するには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 および 2 を指定して、信頼できる各キーの認証キーを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。

コマンド	説明
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

num-packets

SLA 動作中に送信される要求パケットの数を指定するには、SLA モニタ プロトコル コンフィギュレーション モードで **num-packets** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

num-packets *number*

no num-packets *number*

構文の説明

number	SLA 動作中に送信されるパケットの数。有効な値は、1 ～ 100 です。

デフォルト

エコー タイプの場合に送信されるデフォルトのパケット数は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケット損失のために到達可能性情報が不正確になるのを防ぐには、送信されるデフォルトのパケット数を増やします。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

object-group

コンフィギュレーションの最適化に使用できるオブジェクト グループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。コンフィギュレーションからオブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* [**tcp** | **udp** | **tcp-udp**]

no object-group service *obj_grp_id* [**tcp** | **udp** | **tcp-udp**]

構文の説明

icmp-type	echo や echo-reply など ICMP タイプのグループを定義します。メインの **object-group icmp-type** コマンドを入力した後、**icmp-object** コマンドおよび **group-object** コマンドで ICMP オブジェクトを ICMP タイプ グループに追加します。
network	ホストまたはサブネットの IP アドレスのグループを定義します。メインの **object-group network** コマンドを入力した後、**network-object** コマンドおよび **group-object** コマンドでネットワーク オブジェクトをネットワーク グループに追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。
protocol	TCP や UDP などプロトコルのグループを定義します。メインの **object-group protocol** コマンドを入力した後、**protocol-object** コマンドと **group-object** コマンドを使用して、プロトコル オブジェクトをプロトコル グループに追加します。
service	拡張サービス オブジェクト グループの定義には、TCP サービス、UDP サービス、ICMP-type サービス、および（コマンドラインに **tcp**、**udp**、または **tcp-udp** が指定されていない場合には）プロトコルを混在させることができます。メインの **object-group service** コマンドを入力した後、**service-object** コマンドと **group-object** コマンドを使用して、サービス オブジェクトをサービス グループに追加します。 **tcp**、**udp**、または **tcp-udp** が任意でコマンドラインに指定されている場合、**service** には「eq smtp」や「range 2000 2010」など TCP/UDP ポート仕様の標準のサービス オブジェクト グループを定義します。この場合、メインの **object-group service** コマンドを入力した後、**port-object** コマンドと **group-object** コマンドを使用して、ポート オブジェクトをサービス グループに追加します。
tcp	サービス グループが TCP に使用されることを指定します。
tcp-udp	サービス グループが TCP および UDP に使用できることを指定します。
udp	サービス グループが UDP に使用されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　ホスト、プロトコル、サービスなどのオブジェクトを 1 つのグループにまとめてから、そのグループ名を使用して、グループ内の各項目に適用する単一のコマンドを発行できます。

object-group コマンドでグループを定義してから任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはグループ内の各項目に適用されます。この機能を使用すると、コンフィギュレーションのサイズを大幅に削減できます。

オブジェクト グループを定義したときは、適用可能なすべてのセキュリティ アプライアンス コマンドで次のようにグループ名の前に **object-group** キーワードを使用する必要があります。

```
hostname# show running-config object-group group_name
```

group_name はグループの名前です。

次に、オブジェクト グループを定義してから使用する例を示します。

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

また、**access-list** コマンド引数をグループ化できます。

個々の引数	オブジェクト グループの置き換え
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドを階層的にグループ化できます。つまり、オブジェクト グループを別のオブジェクト グループのメンバーにすることができます。

オブジェクト グループを使用するには、次の手順を実行する必要があります。

- すべてのコマンドで次のようにオブジェクト グループ名の前に **object-group** キーワードを使用します。

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group locals
  object-group eng_svc
  ```

  remotes および *locals* は、サンプルのオブジェクト グループ名です。

- オブジェクト グループは空にできません。

- コマンドで現在使用されているオブジェクト グループは削除することも、空にすることもできません。

メインの **object-group** コマンドを入力した後、コマンド モードは対応するモードに変わります。オブジェクト グループは、変更後のモードに定義されます。アクティブ モードは、コマンド プロンプト形式で示されます。たとえば、コンフィギュレーション ターミナル モードのプロンプトは、次のように表示されます。

```
hostname(config)#
```

ここで *hostname* は、セキュリティ アプライアンスの名前です。

ただし、**object-group** コマンドを入力すると、プロンプトは次のように表示されます。

```
hostname(config-type)#
```

ここで *hostname* はセキュリティ アプライアンスの名前で、*type はオブジェクト グループのタイプです。*

object-group モードを終了し、メインの **object-group** コマンドを実行するには、**exit** か **quit**、あるいは **access-list** などその他の有効なコンフィギュレーション モード コマンドを使用します。

show running-config object-group コマンドは、定義済みのすべてのオブジェクト グループを、**show running-config object-group** *grp_id* コマンドが入力されたときには *grp_id* 別に表示し、**show running-config object-group** *grp_type* コマンドが入力されたときにはグループ タイプ別に表示します。**show running-config object-group** コマンドを引数なしで入力すると、定義済みのすべてのオブジェクト グループが表示されます。

以前に定義した **object-group** コマンドのグループを削除するには、**clear configure object-group** コマンドを使用します。引数なしで **clear configure object-group** コマンドを使用すると、コマンドに現在使用されていない定義済みのすべてのオブジェクト グループを削除できます。*grp_type* 引数は、そのグループ タイプのみを対象に、コマンドに使用されていない定義済みのすべてのオブジェクト グループを削除します。

show running-config や **clear configure** など他のすべてのセキュリティ アプライアンス コマンドをオブジェクト グループ モードで使用できます。

オブジェクト グループ モード内のコマンドは、**show running-config object-group**、**write**、または **config** コマンドによって表示または保存されるときにインデントされます。

オブジェクト グループ モード内のコマンドは、コマンド特権レベルがメインのコマンドと同じレベルになります。

access-list コマンドで複数のオブジェクト グループを使用するときには、コマンドに使用されるすべてのオブジェクト グループの要素がリンクされます。最初のグループの要素が 2 つめのグループの要素とリンクされ、続いて最初と 2 つめのグループの要素がともに 3 つのグループの要素にリンクされ、以後同じようにリンクされます。

説明テキストの開始位置は、**description** キーワードに続くスペース（ブランクまたはタブ）の直後の文字となります。

例

次に、**オブジェクト グループ ICMP-type** モードを使用して、新規に ICMP-type オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

次に、**object-group network** コマンドを使用して、新規にネットワーク オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

次に、**object-group network** コマンドを使用して、新規にネットワーク オブジェクト グループを作成し、それを既存のオブジェクト グループにマッピングする例を示します。

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

次に、**オブジェクト グループ プロトコル** モードを使用して、新規にプロトコル オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

次に、**オブジェクト グループ サービス** モードを使用して、新規にポート（サービス）オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

次に、オブジェクト グループに対してテキスト説明を追加および削除する例を示します。

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

次に、**グループ オブジェクト** モードを使用して、以前に定義したオブジェクトで構成されているオブジェクト グループを新規に作成する例を示します。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
```

```
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを指定しないときは、*host_grp_1* および *host_grp_2* にすでに定義されているすべての IP アドレスが含まれるように、*all_hosts* グループを定義する必要があります。**group-object** コマンドを指定すると、重複するホストの定義が削除されます。

次に、オブジェクト グループを使用して、アクセス リスト コンフィギュレーションを簡素化する例を示します。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 209.165.200.225
hostname(config-network)# network-object host 209.165.200.230
hostname(config-network)# network-object host 209.165.200.235
hostname(config-network)# network-object host 209.165.200.240

hostname(config)# object-group service eng_svc tcp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

グループ化を使用しないとアクセス リストの設定には 24 行必要ですが、このグループ化により、1 行で設定できます。グループ化を使用した場合、アクセス リスト コンフィギュレーションは次のようになります。

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

次に、**service-object** サブコマンドを使用する例を示します。このサブコマンドは、TCP サービスおよび UDP サービスをグループ化する場合に便利です。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host host 209.165.200.225
hostname(config-network)# network-object host host 209.165.200.230
hostname(config-network)# network-object host host 209.165.200.235
hostname(config-network)# network-object host host 209.165.200.240

hostname(config)# object-group service usr_svc
hostname(config-service)# service-object tcp eq www
hostname(config-service)# service-object tcp eq https
hostname(config-service)# service-object tcp eq pop3
hostname(config-service)# service-object udp eq ntp
hostname(config-service)# service-object udp eq domain

hostname(config)# access-list acl permit object-group usr_svc object-group locals
object-group remote
```

（注）　**show running-config object-group** コマンドおよび **write** コマンドを使用すると、オブジェクト グループ名で設定したとおりにアクセス リストを表示できます。**show access-list** コマンドは、オブジェクト グループ化なしで個々のエントリに展開されるアクセス リスト エントリを表示します。

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

ocsp disable-nonce

ナンス拡張をディセーブルにするには、クリプト CA トラストポイント コンフィギュレーション モードで **ocsp disable-nonce** コマンドを使用します。デフォルトでは、OCSP 要求にナンス拡張が含まれています。ナンス拡張は、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。ただし、OCSP サーバによっては、この一致するナンス拡張が含まれていない事前生成の応答が使用される場合があります。このようなサーバで OCSP を使用するには、ナンス拡張をディセーブルにする必要があります。ナンス拡張を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

ocsp disable-nonce

no ocsp disable-nonce

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、OCSP 要求にナンス拡張が含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するとき、OCSP 要求には OCSP ナンス拡張が含まれず、セキュリティ アプライアンスは OCSP ナンス拡張をチェックしません。

例

次に、newtrust というトラストポイントのナンス拡張をディセーブルにする例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp disable-nonce
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。

コマンド	説明
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

ocsp url

クライアント証明書の AIA 拡張で指定されたサーバではなく、セキュリティ アプライアンスの OCSP サーバを、トラストポイントに関連付けられたすべての証明書のチェックに使用するように設定するには、暗号 CA トラストポイント コンフィギュレーション モードで **ocsp url** コマンドを使用します。このサーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*

no ocsp url

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、HTTP URL のみをサポートし、トラストポイントごとに URL を 1 つだけ指定できます。

セキュリティ アプライアンスでは 3 つの方法で OCSP サーバの URL を定義でき、その定義方法に従って次の順序で OCSP サーバの使用を試みます。

- **match certificate** コマンドで設定された OCSP サーバ。
- **ocsp url** コマンドで設定された OCSP サーバ。
- クライアント証明書の AIA フィールドに指定された OCSP サーバ。

match certificate コマンドまたは **ocsp url** コマンドで OCSP URL を設定しないと、セキュリティ アプライアンスはクライアント証明書の AIA 拡張に指定された OCSP サーバを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

次に、URL http://10.1.124.22 で OCSP サーバを設定する例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp url http://10.1.124.22
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

onscreen-keyboard

ログイン/パスワード要件とともにオンスクリーン キーボードをログイン ペインまたはすべてのペインに挿入するには、webvpn モードで **onscreen-keyboard** コマンドを使用します。以前に設定したオンスクリーン キーボードを削除するには、このコマンドの **no** 形式を使用します。

onscreen-keyboard {logon | all}

no onscreen-keyboard [logon | all]

構文の説明

logon	ログイン ペインのオンスクリーン キーボードを挿入します。
all	ログイン/パスワードの要件とともに、ログイン ペインおよび他のすべてのペインのオンスクリーン キーボードを挿入します。

デフォルト

オンスクリーン キーボードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

オンスクリーン キーボードを使用すると、キーストロークなしでユーザ クレデンシャルを入力できます。

例

次に、ログイン ページのオンスクリーン キーボードをイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# onscreen-keyboard logon
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn モードを開始し、クライアントレス SSLVPN 接続の属性を設定できるようにします。

ospf authentication

OSPF 認証の使用をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf authentication** コマンドを使用します。デフォルトの認証状態に戻すには、このコマンドの **no** 形式を使用します。

ospf authentication [**message-digest** | **null**]

no ospf authentication

構文の説明

message-digest	（任意）OSPF メッセージ ダイジェスト認証を使用することを指定します。
null	（任意）OSPF 認証を使用しないことを指定します。

デフォルト

デフォルトでは、OSPF 認証はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。**message-digest** キーワードを使用する場合は、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージ ダイジェスト キーを設定します。

下位互換性を確保するため、エリアの認証タイプは引き続きサポートされます。インターフェイスの認証タイプを指定しないと、エリアの認証タイプが使用されます（エリアのデフォルトはヌル認証です）。

このコマンドをオプションなしで使用すると、簡易パスワード認証がイネーブルになります。

例

次に、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする例を示します。

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

関連コマンド

コマンド	説明
ospf authentication-key	ネイバー ルーティング デバイスで使用されるパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

ネイバー ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

ospf authentication-key *password*

no ospf authentication-key

構文の説明

password	ネイバー ルーティング デバイスで使用される OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字間にブランクを含めることができます。パスワードの先頭または末尾のブランクは無視されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドが作成するパスワードは、ルーティング プロトコル パケットの送信時に、OSPF ヘッダーに直接挿入されるキーとして使用されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

例

次に、OSPF 認証のパスワードを指定する例を示します。

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイス経由でパケットを送信するコストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイス コストをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ospf cost *interface_cost*

no ospf cost

構文の説明

interface_cost	インターフェイス経由でパケットを送信するコスト（リンクステート メトリック）。これは、符号なし整数値 0 ～ 65535 です。0 はインターフェイスに直接接続されているネットワークを表し、インターフェイス帯域幅が大きくなるほど、そのインターフェイス経由のパケット送信に伴うコストは低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。 セキュリティ アプライアンスでの OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファスト イーサネットおよびギガビット イーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

デフォルト

デフォルトの *interface_cost* は、10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでパケットを送信するコストを明示的に指定できます。*interface_cost* パラメータは、符号なし整数値 0 ～ 65535 です。

no ospf cost コマンドを使用すると、パス コストをデフォルト値にリセットできます。

例

次に、選択したインターフェイスでパケットを送信するコストを指定する例を示します。

```
hostname(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定したインターフェイスの設定を表示します。

ospf database-filter

同期およびフラッディング時に OSPF インターフェイスへの発信 LSA をすべてフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter all out

no ospf database-filter all out

構文の説明

all out	OSPF インターフェイスへの発信 LSA をすべてフィルタリングします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA の転送を復元します。

例

次に、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする例を示します。

```
hostname(config-if)# ospf database-filter all out
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf dead-interval *seconds*

no ospf dead-interval

構文の説明

seconds	hello パケットが確認されない時間の長さ。*seconds* のデフォルトは、**ospf hello-interval** コマンドによって設定される間隔（1 ～ 65535）の 4 倍です。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドによって設定される間隔の 4 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（no hello パケットが確認されない時間の長さ）を設定できます。*seconds* 引数にはデッド間隔を指定し、その値はネットワーク上のすべてのノードで同じである必要があります。*seconds* のデフォルトは、**ospf hello-interval** コマンドによって設定される間隔（1 ～ 65535）の 4 倍です。

no ospf dead-interval コマンドは、デフォルトの間隔値を復元します。

例

次に、OSPF デッド間隔を 1 分に設定する例を示します。

```
hostname(config-if)# ospf dead-interval 60
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイス上での hello パケットの送信間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf hello-interval

インターフェイス上での hello パケットの送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf hello-interval *seconds*

no ospf hello-interval

構文の説明

seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

デフォルト

hello-interval *seconds* のデフォルト値は、10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次に、OSPF hello 間隔を 5 秒に設定する例を示します。

```
hostname(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf message-digest-key

OSPF MD5 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf message-digest-key** コマンドを使用します。MD5 キーを削除するには、このコマンドの **no** 形式を使用します。

ospf message-digest-key *key-id* **md5** *key*

no ospf message-digest-key

構文の説明

key-id	MD5 認証をイネーブルにし、認証キー ID 番号を数値で指定します。有効な値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字のパスワード。キーの文字間にスペースを含めることができます。キーの先頭または末尾のスペースは無視されます。MD5 認証は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。このコマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、認証キーを識別する 1 ～ 255 の数値です。*key* は、最大 16 バイトの英数字のパスワードです。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。

例

次に、OSPF 認証の MD5 キーを指定する例を示します。

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

関連コマンド

コマンド	説明
area authentication	OSPF エリア認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf mtu-ignore

受信データベース パケットで OSPF 最大伝送単位（MTU）ミスマッチ検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore

no ospf mtu-ignore

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、**ospf mtu-ignore** はイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが Database Descriptor（DBD; データベース記述子）パケットを交換するときに実行されます。DBD パケットの受信 MTU が、着信インターフェイスに設定されている IP MTU よりも高くなっている場合、OSPF 隣接は確立されません。**ospf mtu-ignore** コマンドは、受信 DBD パケットで OSPF MTU ミスマッチ検出をディセーブルにします。デフォルトではイネーブルです。

例

次に、**ospf mtu-ignore** コマンドをディセーブルにする例を示します。

```
hostname(config-if)# ospf mtu-ignore
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf network point-to-point non-broadcast

OSPF インターフェイスをポイントツーポイントの非ブロードキャスト ネットワークとして設定するには、インターフェイス コンフィギュレーション モードで **ospf network point-to-point non-broadcast** コマンドを使用します。コンフィギュレーションからこのコマンドを削除するには、このコマンドの **no** 形式を使用します。**ospf network point-to-point non-broadcast** コマンドを使用すると、VPN トンネルで OSPF ルートを送信できます。

ospf network point-to-point non-broadcast

no ospf network point-to-point non-broadcast

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをポイントツーポイントとして指定したときは、OSPF ネイバーを手動で設定する必要があります。ダイナミック探索は機能しません。OSPF ネイバーを手動で設定するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。

インターフェイスをポイントツーポイントとして設定したときには、次の制約事項が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。
- ネイバーを明示的に設定しない限り、インターフェイスは隣接を形成できません。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、その同じインターフェイスでは上流のルータがある通常の OSPF を実行できません。
- OSPF 更新が VPN トンネルを通過できるように、OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後でクリプト マップをインターフェイスにバインドした場合は、OSPF 隣接を VPN トンネル経由で確立できるように、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。

例

次に、選択したインターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして設定する例を示します。

```
hostname(config-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定した OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータのプライオリティを変更するには、インターフェイス コンフィギュレーション モードで **ospf priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

ospf priority *number*

no ospf priority [*number*]

構文の説明

number	ルータのプライオリティを指定します。有効な値は、0 ～ 255 です。

デフォルト

number のデフォルト値は、1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。ルータのプライオリティは、マルチアクセス ネットワークへのインターフェイス専用に設定されます（つまり、ポイントツーポイント ネットワークへのインターフェイスには設定されません）。

例

次に、選択したインターフェイスで OSPF プライオリティを変更する例を示します。

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接の LSA 再送信間の時間を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

構文の説明

seconds	インターフェイスに属する隣接ルータの LSA 再送信間の時間を指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

retransmit-interval *seconds* のデフォルト値は、5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答メッセージを受信しないと、ルータは LSA を再送信します。

このパラメータの設定値は控えめにする必要があります。そうしないと、不要な再送信が発生します。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次に、LSA の再送信間隔を変更する例を示します。

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

構文の説明

seconds	インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を設定します。デフォルト値は 1 秒で、有効な値の範囲は 1 ～ 65535 秒です。

デフォルト

seconds のデフォルト値は、1 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

更新パケット内の LSA には、送信前に、*seconds* 引数で指定した値によって増加された経過時間が格納されます。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。

リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。この設定は、非常に低速のリンクでより重要な意味を持ちます。

例

次に、選択したインターフェイスの送信遅延を 3 秒に設定する例を示します。

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

otp expiration

ローカル Certificate Authority（CA; 認証局）登録ページ用に発行されたワンタイム パスワード（OTP）の有効期間を時間単位で指定するには、CA サーバ コンフィギュレーション モードで **otp expiration** コマンドを使用します。期間をデフォルトの時間数にリセットするには、このコマンドの **no** 形式を使用します。

otp expiration *timeout*

no otp expiration

構文の説明

timeout	登録ページ用の OTP が期限切れになる前に、ユーザがローカル CA から証明書を登録する必要がある期間を時間単位で指定します。有効な値の範囲は、1 ～ 720 時間（30 日）です。

デフォルト

デフォルトでは、証明書登録用の OTP の有効期限は 72 時間（3 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

OTP の有効期限には、ユーザが CA サーバの登録ページにログインする必要がある時間数を指定します。ユーザがログインし、証明書を登録すると、**enrollment retrieval** コマンドで指定された期間が開始されます。

（注） 登録インターフェイス ページで証明書を登録するためのユーザ OTP は、そのユーザの発行済みの証明書とキー ペアが含まれている PKCS12 ファイルをアンロックするためのパスワードとしても使用されます。

例

次に、登録ページ用の OTP が 24 時間適用されることを指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# otp expiration 24
hostname(config-ca-server)#
```

次に、OTP 期間をデフォルトの 72 時間にリセットする例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server))# no otp expiration
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
enrollment-retrieval	登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server	認証局コンフィギュレーションを表示します。

outstanding

認証されていない電子メール プロキシ セッションの数を制限するには、適用可能な電子メール プロキシ コンフィギュレーション モードで **outstanding** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

outstanding {*number*}

no outstanding

構文の説明

number	認証されていないセッションを許可する数。範囲は 1 ～ 1000 です。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

認証されていないセッションを許可する数に制限がないコンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。これは、電子メール ポートに対する DoS 攻撃も制限します。

電子メール プロキシ接続には、3 つの状態があります。

1. 新規に電子メール接続が確立されると、「認証されていない」状態になります。
2. この接続でユーザ名が提示されると、「認証中」状態になります。
3. セキュリティ アプライアンスが接続を認証すると、「認証済み」状態になります。

認証されていない状態の接続の数が設定済みの制限値を超えた場合、セキュリティ アプライアンスは認証されていない接続のうち最も古いものを終了して、過負荷を回避します。認証済みの接続は終了しません。

例

次に、POP3S 電子メール プロキシの認証されていないセッションの制限を 12 に設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

override-account-disable

AAA サーバからの account-disabled インジケータを上書きするには、トンネル グループ一般属性コンフィギュレーション モードで **override-account-disable** コマンドを使用します。上書きをディセーブルにするには、このコマンドの **no** 形式を使用します。

override-account-disable

no override-account-disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT LDAP がある RADIUS や Kerberos など、「account-disabled」インジケータを返すサーバに有効です。

IPSec RA および WebVPN トンネル グループにこの属性を設定できます。

例

次に、「testgroup」という WebVPN トンネル グループについて AAA サーバからの「account-disabled」インジケータの上書きを許可する例を示します。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

次に、「QAgroup」という IPSec リモート アクセス トンネル グループについて AAA サーバからの「account-disabled」インジケータの上書きを許可する例を示します。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	特定のトンネル グループのトンネル グループ データベースまたはコンフィギュレーションをクリアします。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

override-svc-download

AnyConnect クライアントまたは SSL VPN クライアントをダウンロードするためのグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きするように接続プロファイルを設定するには、トンネル グループ webvpn 属性コンフィギュレーション モードで **override-svc-download** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

override-svc-download enable

no override-svc-download enable

デフォルト

デフォルトではディセーブルになっています。セキュリティ アプライアンスは、クライアントをダウンロードするためのグループ ポリシーまたはユーザ名属性コンフィギュレーションを上書きしません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、**vpn-tunnel-protocol** コマンドによってグループ ポリシーまたはユーザ名属性でクライアントレスか SSL VPN またはその両方がイネーブルになっているかどうかに基づいて、リモート ユーザに対してクライアントレス接続、AnyConnect 接続、または SSL VPN クライアント接続を許可します。**svc ask** コマンドはさらに、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザに要求して、クライアントのユーザ エクスペリエンスを変更します。

ただし、特定のトンネル グループのもとでログインしているクライアントレス ユーザが、ダウンロードの要求が期限切れになってクライアントレス SSL VPN ホームページが表示されるまで待たなくてもよいようにすることを推奨します。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザには、**vpn-tunnel-protocol** コマンドまたは **svc ask** コマンドの設定に関係なく、ただちにクライアントレス SSL VPN ホームページが表示されるようになります。

例

次の例では、ユーザは接続プロファイル *engineering* のトンネル グループ webvpn 属性コンフィギュレーション モードを開始し、この接続プロファイルでクライアントのダウンロード要求に関するグループ ポリシーおよびユーザ名属性の設定を上書きしています。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

CHAPTER 22

packet-tracer コマンド～ pwd コマンド

packet-tracer

パケット スニッフィングおよびネットワーク障害隔離を実行するパケット トレース機能をイネーブルにするには、特権 EXEC コンフィギュレーション モードで **packet-tracer** コマンドを使用します。パケット キャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

packet-tracer input [*src_int*] *protocol src_addr src_port dest_addr dest_port* [**detailed**] [**xml**]

no packet-tracer

構文の説明

input *src_int*	パケット トレースの送信元インターフェイスを指定します。
protocol	パケット トレースのプロトコル タイプを指定します。使用可能なプロトコル タイプ キーワードは、*icmp*、*rawip*、*tcp*、または *udp* です。
src_addr	パケット トレースの送信元アドレスを指定します。
src_port	パケット トレースの送信元ポートを指定します。
dest_addr	パケット トレースの宛先アドレスを指定します。
dest_port	パケット トレースの宛先ポートを指定します。
detailed	（任意）パケット トレースの詳細情報を提供します。
xml	（任意）トレース キャプチャを XML 形式で表示します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケットのキャプチャに加えて、セキュリティ アプライアンスを介してパケットの寿命をトレースして、想定どおりに動作しているかどうかを確認できます。**packet-tracer** コマンドを使用すると、次の操作を実行できます。

- 実働ネットワークにおけるすべてのパケット ドロップをデバッグします。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルールと、ルールの追加に使用した CLI ラインを表示します。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。

packet-tracer コマンドは、パケットに関する詳細情報、およびセキュリティ アプライアンスによるパケットの処理方法を提供します。コンフィギュレーションからのコマンドでパケットがドロップしなかった場合、**packet-tracer** コマンドは、原因に関する情報を判読しやすい方法で提供します。たとえば、無効なヘッダー検証が原因でパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」というメッセージが表示されます。

例

内部ホスト 10.2.25.3 から外部ホスト 209.165.202.158 へのパケット トレーシングをイネーブルにし、詳細情報を出力するには、次のように入力します。

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

page style

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **page style** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

page style *value*

[**no**] **page style** *value*

構文の説明

value	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータ（最大 256 文字）。

デフォルト

デフォルトのページ スタイルは、background-color:white;font-family:Arial,Helv,sans-serif です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ページ スタイルを large にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
title	WebVPN ページのタイトルをカスタマイズします。

pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりのデフォルト行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

pager [lines] *lines*

構文の説明

[**lines**] *lines*	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、特権 EXEC モードのコマンドからグローバル コンフィギュレーション モードのコマンドに変更されました。**terminal pager** コマンドが、特権 EXEC モードのコマンドとして追加されました。

使用上のガイドライン

このコマンドは、Telnet セッションでのデフォルトの pager line 設定を変更します。現在のセッションについてのみ、設定を一時的に変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキストに対して Telnet 接続し、他のコンテキストに変更した場合、そのコンテキストの **pager** コマンドで別の設定が使用される場合でも、pager line 設定はセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次に、表示される行数を 20 に変更する例を示します。

```
hostname(config)# pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージを Telnet セッションで表示できるようにします。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

parameters

パラメータ コンフィギュレーション モードを開始してインスペクション ポリシー マップのパラメータを設定するには、ポリシー マップ コンフィギュレーション モードで **parameters** コマンドを使用します。

parameters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で、**inspect** コマンドを使用してインスペクション エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシー マップで定義されているアクションを、オプションでイネーブルにすることもできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、1 つ以上の **parameters** コマンドをサポートできます。パラメータは、インスペクション エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

例

次に、デフォルトのインスペクション ポリシー マップにおける DNS パケットの最大メッセージ長を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

participate

デバイスを仮想ロード バランシング クラスタに強制参加させるには、VPN ロード バランシング コンフィギュレーション モードで **participate** コマンドを使用します。クラスタへの参加からデバイスを削除するには、このコマンドの **no** 形式を使用します。

participate

no participate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作では、デバイスは VPN ロード バランシング クラスタに参加しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**interface** および **nameif** コマンドを使用してインターフェイスを設定し、**vpn load-balancing** コマンドを使用して VPN ロード バランシング モードを開始する必要があります。さらに、**cluster ip** コマンドを使用してクラスタ IP アドレスを設定し、仮想クラスタ IP アドレスが参照するインターフェイスを設定しておく必要があります。

このコマンドは、このデバイスを仮想ロード バランシング クラスタに強制的に参加させます。デバイスへの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

クラスタに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。

（注） 暗号化を使用するときは、**isakmp enable** *inside* コマンドをあらかじめ設定しておく必要があります。*inside* は、ロード バランシングの内部インターフェイスを指定します。ロード バランシングの内部インターフェイスで isakmp がイネーブルでない場合は、クラスタ暗号化を設定しようとするとエラー メッセージが表示されます。

isakmp が **cluster encryption** コマンドの設定時にはイネーブルで、**participate** コマンドを設定する前にディセーブルになった場合、**participate** コマンドを入力するとエラー メッセージが表示され、ローカル デバイスはクラスタに参加しません。

例

次に、現在のデバイスを VPN ロード バランシング クラスタに参加できるようにする **participate** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

passive-interface

インターフェイスで RIP ルーティング更新の送信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスで RIP ルーティング更新を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

構文の説明

default	（任意）すべてのインターフェイスを受動モードに設定します。
if_name	（任意）指定したインターフェイスをパッシブ モードに設定します。

デフォルト

RIP がイネーブルになると、アクティブ RIP に対してすべてのインターフェイスがイネーブルになります。

インターフェイスまたは **default** キーワードを指定しない場合、コマンドのデフォルトは **default** であり、コンフィギュレーションでは `passive-interface default` として表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス上でパッシブ RIP をイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを設定しますが、ルーティング更新はブロードキャストしません。

例

次に、外部インターフェイスをパッシブ RIP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、RIP 更新を送受信します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドをクリアします。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。
show running-config rip	実行コンフィギュレーションの RIP コマンドを表示します。

passive-interface（EIGRP）

インターフェイスで EIGRP ルーティング更新の送受信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスでルーティング更新を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

構文の説明

default	（任意）すべてのインターフェイスを受動モードに設定します。
if_name	（任意）**nameif** コマンドでパッシブ モードに指定したインターフェイスの名前。

デフォルト

そのインターフェイスでルーティングがイネーブルになると、アクティブ ルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスがイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	EIGRP ルーティングのサポートが追加されました。

使用上のガイドライン

インターフェイス上でパッシブ ルーティングをイネーブルにします。EIGRP の場合は、これによりそのインターフェイスでのルーティング更新の送受信がディセーブルになります。

EIGRP コンフィギュレーションでは、複数の **passive-interface** コマンドを使用できます。**passive-interface default** コマンドを使用してすべてのインターフェイスで EIGRP ルーティングをディセーブルにし、次に **no passive-interface** コマンドを使用して特定インターフェイスで EIGRP ルーティングをイネーブルにすることが可能です。

例

次に、外部インターフェイスをパッシブ EIGRP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、EIGRP 更新を送受信します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

次に、内部インターフェイスを除くすべてのインターフェイスをパッシブ EIGRP に設定する例を示します。内部インターフェイスのみが EIGRP 更新を送受信します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface default
hostname(config-router)# no passive-interface inside
```

関連コマンド

コマンド	説明
show running-config router	実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。

passwd

ログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** コマンドを使用します。パスワードをデフォルトの「cisco」に戻すには、このコマンドの **no** 形式を使用します。Telnet または SSH を使用してデフォルト ユーザとして CLI にアクセスするときに、ログイン パスワードを求められます。ログイン パスワードを入力すると、ユーザ EXEC モードが開始されます。

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

構文の説明

encrypted	（任意）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。
passwd | **password**	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。
password	パスワードを最大 80 文字のストリングで設定します。大文字と小文字は区別されます。パスワードにスペースを含めることはできません。

デフォルト

デフォルトのパスワードは「cisco」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このログイン パスワードは、デフォルト ユーザのものです。**aaa authentication console** コマンドを使用して Telnet または SSH のユーザごとに CLI 認証を設定する場合、このパスワードは使用されません。

例

次に、パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# passwd Pa$$w0rd
```

次に、パスワードを別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定する例を示します。

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードをクリアします。
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config passwd	暗号化された形式でログイン パスワードを表示します。

password（クリプト CA トラスト ポイント）

登録時に CA に登録されたチャレンジ フレーズを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **password** コマンドを使用します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

password *string*

no password

構文の説明

string	パスワードの名前をストリングとして指定します。最初の文字を数値にはできません。ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字 - スペース - 任意の文字の形式ではパスワードを指定できません。数字の後にスペースを使用すると、問題が発生します。たとえば、「hello 21」は適切なパスワードですが、「21 hello」はそうではありません。パスワード チェックでは、大文字と小文字が区別されます。たとえば、パスワード「Secret」は、パスワード「secret」とは異なります。

デフォルト

デフォルト設定では、パスワードを含めません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書失効パスワードを指定できます。指定されたパスワードは、更新されたコンフィギュレーションがセキュリティ アプライアンスによって NVRAM に書き込まれるときに暗号化されます。

このコマンドがイネーブルの場合、証明書登録時にパスワードを求められません。

例

次に、トラストポイント central に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に対する登録要求で CA に登録されたチャレンジ フレーズを指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

password-management

パスワード管理をイネーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **password-management** コマンドを使用します。パスワード管理をディセーブルにするには、このコマンドの **no** 形式を使用します。日数をデフォルト値にリセットするには、このコマンドの **no** 形式を使用し、**password-expire-in-days** キーワードを指定します。

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

構文の説明

days	現行のパスワードが失効するまでの日数（0 ～ 180）を指定します。**password-expire-in-days** キーワードを指定する場合は、このパラメータは必須です。
password-expire-in-days	（任意）直後のパラメータが、セキュリティ アプライアンスでユーザに対して失効が迫っている警告を開始してから、現行のパスワードが失効するまでの日数を指定していることを示します。このオプションは、LDAP サーバに対してのみ有効です。詳細については、「Usage Notes」を参照してください。

デフォルト

このコマンドを指定しない場合は、パスワード管理が発生しません。**password-expire-in-days** キーワードを指定しない場合、現行のパスワードが失効する前に警告を開始するデフォルトの期間は、14 日です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPSec リモート アクセスおよび SSL VPN トンネル グループのパスワード管理を設定できます。

password-management コマンドを設定すると、セキュリティ アプライアンスは、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それからセキュリティ アプライアンスは、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、そのような通知をサポートする AAA サーバに対して有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

（注）　MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。

セキュリティ アプライアンスのリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPSec VPN クライアント
- クライアントレス SSL VPN

Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート*されません*。RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、セキュリティ アプライアンスからは RADIUS サーバのみに対して通信しているように見えます。

（注）　LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、セキュリティ アプライアンスでは Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

このコマンドは、パスワードが失効するまでの日数を変更するものではなく、セキュリティ アプライアンスがユーザに対してパスワード失効の警告を開始してから失効するまでの日数を変更するものである点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。

例

次に、WebVPN トンネル グループ「testgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数を 90 に設定する例を示します。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

次に、IPSec リモート アクセス トンネル グループ「QAgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数としてデフォルトの 14 日を使用する例を示します。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
```

```
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードをクリアします。
passwd	ログイン パスワードを設定します。
radius-with-expiry	RADIUS 認証時のパスワード更新のネゴシエーションをイネーブルにします（廃止）。
show running-config passwd	暗号化された形式でログイン パスワードを表示します。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

password-parameter

SSO 認証用のユーザ パスワードを送信する HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **password-parameter** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

password-parameter *string*

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	HTTP POST 要求に含まれるパスワード パラメータの名前。パスワードの最大長は 128 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、認証 Web サーバにシングル サインオン認証要求を送信します。必須のコマンド **password-parameter** では、POST 要求に SSO 認証用のユーザ パスワード パラメータを含める必要があることを指定します。

（注）　ユーザは、ログイン時に実際のパスワード値を入力します。このパスワード値は POST 要求に入力され、認証 Web サーバに渡されます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、user_password という名前のパスワード パラメータを指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

password-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **password-prompt** コマンドを使用します。

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

パスワード プロンプトのデフォルト テキストは、「PASSWORD:」です。

パスワード プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、テキストを「Corporate Password:」に変更し、フォントのウェイトを太くするようにデフォルト スタイルを変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# password-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# password-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

password-storage

ユーザがクライアント システムに各自のログイン パスワードを保管できるようにするには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワードの保管をディセーブルにするには、**password-storage disable** コマンドを使用します。

実行コンフィギュレーションから password-storage 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから password-storage 値を継承できます。

password-storage {enable | disable}

no password-storage

構文の説明

disable	パスワードの保管をディセーブルにします。
enable	パスワードの保管をイネーブルにします。

デフォルト

パスワードの保管はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

例

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

ピアの証明書を使用してピアの ID を検証するかどうかを指定するには、トンネル グループ IPSec 属性モードで **peer-id-validate** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

peer-id-validate *option*

no peer-id-validate

構文の説明

option	次のいずれかのオプションを指定します。 • **req**：必須 • **cert**：証明書でサポートされる場合 • **nocheck**：チェックしない

デフォルト

このコマンドのデフォルト設定は、**req** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

例

次に、設定 IPSec コンフィギュレーション モードで、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループ用のピア証明書の ID を使用してピアの検証を要求する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。

コマンド	説明
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

構文の説明

verbose	パフォーマンス モニタ情報をセキュリティ アプライアンス コンソールに表示します。
interval *seconds*	コンソールでパフォーマンス表示がリフレッシュされるまでの秒数を指定します。
quiet	パフォーマンス モニタ表示をディセーブルにします。
settings	間隔、および quiet と verbose のどちらであるかを表示します。
detail	パフォーマンスに関する詳細情報を表示します。

デフォルト

seconds は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。
7.2(1)	**detail** キーワードのサポートが追加されました。

使用上のガイドライン

perfmon コマンドを使用すると、セキュリティ アプライアンスのパフォーマンスをモニタできます。**show perfmon** コマンドを使用すると、ただちに情報が表示されます。**perfmon verbose** コマンドを使用すると、2 分間隔で継続して情報が表示されます。**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを組み合わせて使用すると、指定した秒数の間隔で継続して情報が表示されます。

次に、パフォーマンス情報の表示例を示します。

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s

FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

この情報には、毎秒発生する変換数、接続数、Websense 要求数、アドレス変換数（フィックスアップ数）、AAA トランザクション数が示されます。

例

次に、パフォーマンス モニタ統計情報を 30 秒間隔でセキュリティ アプライアンス コンソールに表示する例を示します。

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

コマンド	説明
show perfmon	パフォーマンス情報を表示します。

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで **periodic** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

構文の説明

days-of-the-week	（任意）1 番めの days-of-the-week 引数は、関連付けられている時間範囲の有効範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。 この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
time	時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。
to	「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。

デフォルト

periodic コマンドで値を入力しない場合は、セキュリティ アプライアンスへのアクセスが **time-range** コマンドで定義されたとおりにただちに有効になり、常に有効になります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲が有効になるタイミングを指定する 1 つの方法です。**absolute** コマンドを使用して絶対時間範囲を指定する、という別の方法もあります。**time-range** グローバル コンフィギュレーション コマンドで時間範囲の名前を指定した後に、これらのコマンドのいずれかを使用します。**time-range** コマンド 1 つあたり複数の **periodic** エントリを使用できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

time-range コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute start** 時刻を経過した後にのみ評価の対象になり、**absolute end** 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、セキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

例

次に例をいくつか示します。

必要な設定	入力内容
月曜～金曜、午前 8 時～ 午後 6 時 only	**periodic weekdays 8:00 to 18:00**
毎日、午前 8 時～ 午後 6 時 only	**periodic daily 8:00 to 18:00**
月曜日午前 8:00 ～ 金曜日午前 8:00 の毎分	**periodic monday 8:00 to friday 20:00**
週末（土曜日の朝～日曜日の夜）	**periodic weekend 00:00 to 23:59**
土曜日と日曜日の正午～深夜	**periodic weekend 12:00 to 23:59**

次に、月曜日から金曜日の午前 8:00 ～ 午後 6:00 に、セキュリティ アプライアンスへのアクセスを 許可する 例を示します。

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

次に、特定の曜日（月曜日、火曜日、および金曜日）の午前 10:30 ～午後 12:30 に、セキュリティ アプライアンスへのアクセスを許可する 例を示します。

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

permit errors

無効な GTP パケットを許可するか、または許可しないと解析が失敗してドロップされるパケットを許可するには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。このモードには **gtp-map** コマンドを使用してアクセスします。デフォルトの動作（無効なパケットまたは解析中に失敗したパケットはすべてドロップされる）に戻すには、このコマンドの **no** 形式を使用します。

permit errors

no permit errors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、無効なパケットまたは解析中に失敗したパケットはすべてドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用すると、無効なパケットやメッセージのインスペクション中にエラーが発生したパケットをドロップするのではなく、セキュリティ アプライアンス経由で送信することができます。

例

次に、解析中に無効なパケットや失敗したパケットを含むトラフィックを許可する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
permit response	ロード バランシング GSN をサポートします。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

permit response

ロード バランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。このモードには **gtp-map** コマンドを使用してアクセスします。セキュリティ アプライアンスで要求の送信先ホスト以外の GSN から GTP 応答をドロップできるようにするには、このコマンドの **no** 形式を使用します。

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

構文の説明

from-object-group *from_obj_group_id*	**object-group** コマンドを使用して設定されたオブジェクト グループの名前を指定します。このオブジェクト グループは、*to_obj_group_id* 引数で指定されたオブジェクト グループ内の GSN セットに応答を送信できます。セキュリティ アプライアンスは、IPv4 アドレスを持つネットワークオブジェクトが含まれたオブジェクトグループのみをサポートしています。現在、IPv6 アドレスは GTP ではサポートされていません。
to-object-group *to_obj_group_id*	**object-group** コマンドを使用して設定されたオブジェクト グループの名前を指定します。このオブジェクト グループは、*from_obj_group_id* 引数で指定されたオブジェクト グループ内の GSN セットから応答を受信できます。セキュリティ アプライアンスは、IPv4 アドレスを持つネットワークオブジェクトが含まれたオブジェクトグループのみをサポートしています。現在、IPv6 アドレスは GTP ではサポートされていません。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、要求の送信先ホスト以外の GSN から GTP 応答をドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0（4）	このコマンドが導入されました。

使用上のガイドライン

ロード バランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。**permit response** コマンドは、GTP 応答の送信先とは異なる GSN からの応答を許可するように GTP マップを設定します。

ロードバランシング GSN のプールは、ネットワーク オブジェクトとして指定します。同様に、SGSN もネットワーク オブジェクトとして指定します。応答している GSN が GTP 要求の送信先の GSN と同じオブジェクト グループに属している場合、および応答している GSN による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN がある場合、セキュリティ アプライアンスはその応答を許可します。

例

次に、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 のホストへの GTP 応答を許可する例を示します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
permit errors	無効な GTP パケットを許可します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

pfs

PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。実行コンフィギュレーションから PFS 属性を削除するには、このコマンドの **no** 形式を使用します。

pfs {enable | disable}

no pfs

構文の説明

disable	PFS をディセーブルにします。
enable	PFS をイネーブルにします。

デフォルト

PFS はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

VPN クライアントとセキュリティ アプライアンスの PFS 設定は一致する必要があります。

別のグループ ポリシーから PFS の値を継承できるようにするには、このコマンドの **no** 形式を使用します。

IPSec ネゴシエーションでは、PFS により、新しい各暗号キーはそれまでのあらゆるキーと無関係であることが保証されます。

例

次に、FirstGroup という名前のグループ ポリシーに対して PFS を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

phone-proxy

電話プロキシ インスタンスを設定するには、グローバル コンフィギュレーション モードで **phone-proxy** コマンドを使用します。

電話プロキシ インスタンスを削除するには、このコマンドの **no** 形式を使用します。

phone-proxy *phone_proxy_name*

no phone-proxy *phone_proxy_name*

構文の説明

phone_proxy_name	Phone Proxy インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

セキュリティ アプライアンスでは、電話プロキシ インスタンスを 1 つだけ設定できます。

HTTP プロキシ サーバ用に NAT が設定されている場合、IP 電話に関する HTTP プロキシ サーバのグローバルまたはマッピング IP アドレスは、電話プロキシ コンフィギュレーション ファイルに書き込まれます。

例

次に、**phone-proxy** コマンドを使用して、電話プロキシ インスタンスを設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
hostname(config-phone-proxy)# media-termination address 128.106.254.3
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
hostname(config-phone-proxy)# timeout secure-phones 00:05:00
hostname(config-phone-proxy)# disable service-settings
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（**Phone-Proxy**）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

pim

インターフェイス上で PIM を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

pim

no pim

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。**pim** コマンドの **no** 形式のみが、コンフィギュレーションに保存されます。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

例

次に、選択したインターフェイスで PIM をディセーブルにする例を示します。

```
hostname(config-if)# no pim
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim accept-register

PIM 登録メッセージをフィルタリングするようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

構文の説明

list *acl*	アクセス リストの名前または番号を指定します。このコマンドでは、拡張ホスト ACL のみを使用します。
route-map *map-name*	ルート マップ名を指定します。参照されるルート マップでは、拡張ホスト ACL を使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、不正な送信元を RP に登録できないようにするために使用します。不正な送信元が RP に登録メッセージを送信すると、セキュリティ アプライアンスはただちに登録停止メッセージを送り返します。

例

次に、「no-ssm-range」という名前のアクセス リストで定義された送信元からの PIM 登録メッセージを制限する例を示します。

```
hostname(config)# pim accept-register list no-ssm-range
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim bidir-neighbor-filter

DF 選出に参加できる双方向対応ネイバーを制御するには、インターフェイス コンフィギュレーション モードで **pim bidir-neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストは、双方向 DF 選出に参加できるネイバーを定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。

デフォルト

すべてのルータは双方向対応であると見なされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

pim bidir-neighbor-filter コマンドを使用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。この場合、すべてのルータのスパース モード ドメインへの参加を許可しながら、DF 選出へ参加しなければならないルータを指定します。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

pim bidir-neighbor-filter コマンドがイネーブルの場合、ACL で許可されているルータは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

例

次に、10.1.1.1 を PIM 双方向ネイバーにできる例を示します。

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

関連コマンド

コマンド	説明
multicast boundary	管理上有効範囲が設定されたマルチキャスト アドレスに対してマルチキャスト境界を定義します。
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim dr-priority

指定ルータ選出に使用されるセキュリティ アプライアンスでネイバーのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*

no pim dr-priority

構文の説明

number	0 ～ 4294967294 までの数字。この番号は、指定ルータを決定するときにデバイスのプライオリティを判断するために使用されます。0 を指定すると、セキュリティ アプライアンスは指定ルータになりません。

デフォルト

デフォルト値は、1 です

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスでプライオリティ値が最大のデバイスが PIM 指定ルータになります。複数のデバイスで指定ルータのプライオリティが同じである場合は、IP アドレスが最大のデバイスが DR になります。デバイスの hello メッセージに DR-Priority Option が含まれていない場合は、プライオリティが最大のデバイスとして扱われ、指定ルータになります。複数のデバイスで hello メッセージにこのオプションが含まれていない場合は、IP アドレスが最大のデバイスが指定ルータになります。

例

次に、インターフェイスの DR プライオリティを 5 に設定する例を示します。

```
hostname(config-if)# pim dr-priority 5
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello-interval をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

構文の説明

seconds	セキュリティ アプライアンスが hello メッセージを送信するまでの待機秒数。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。

デフォルト

30 秒

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PIM hello 間隔を 1 分に設定する例を示します。

```
hostname(config-if)# pim hello-interval 60
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim join-prune-interval

PIM Join/Prune の間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

構文の説明

seconds	セキュリティ アプライアンスが Join/Prune メッセージを送信するまでの待機秒数。有効な値の範囲は、10 ～ 600 秒です。デフォルトは 60 秒です。

デフォルト

60 秒

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PIM Join/Prune 間隔を 2 分に設定する例を示します。

```
hostname(config-if)# pim join-prune-interval 120
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim neighbor-filter

PIM に参加できる隣接ルータを制御するには、インターフェイス コンフィギュレーション モードで **pim neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

構文の説明

acl	アクセス リストの名前または番号を指定します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM に参加できる隣接ルータを定義します。このコマンドがコンフィギュレーションに存在しない場合、制限はありません。

コンフィギュレーションでこのコマンドを使用するには、マルチキャスト ルーティングおよび PIM がイネーブルである必要があります。マルチキャスト ルーティングをディセーブルにすると、このコマンドはコンフィギュレーションから削除されます。

例

次に、IP アドレスが 10.1.1.1 であるルータをインターフェイス GigabitEthernet0/2 で PIM ネイバーにする例を示します。

```
hostname(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
hostname(config)# access-list pim_filter deny any
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim old-register-checksum

古いレジスタ チェックサム方式を使用するランデブー ポイント（RP）での下位互換性を保つには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠レジスタを生成するには、このコマンドの **no** 形式を使用します。

pim old-register-checksum

no pim old-register-checksum

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

セキュリティ アプライアンス は PIM RFC 準拠レジスタを生成します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス ソフトウェアは、Cisco IOS 方式を使用せずに、PIM ヘッダーにチェックサムのあるレジスタ メッセージとそれに続く 4 バイトのみを受け入れます。つまり、すべての PIM メッセージ タイプについて PIM メッセージ全体を含むレジスタ メッセージを受け入れます。**pim old-register-checksum** コマンドを使用すると、Cisco IOS ソフトウェアと互換性のあるレジスタが生成されます。

例

次に、古いチェックサム計算を使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# pim old-register-checksum
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

pim rp-address

PIM ランデブー ポイント（RP）のアドレスを使用するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

構文の説明

acl	（任意）RP とともに使用されるマルチキャスト グループを定義する標準アクセス リストの名前または番号。このコマンドではホスト ACL を使用しないでください。
bidir	（任意）指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定せずにコマンドを設定した場合、指定したグループは PIM スパース モードで動作します。
ip_address	PIM RP になるルータの IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

PIM RP アドレスは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

一般的な PIM Sparse Mode（PIM-SM; PIM スパース モード）内または双方向ドメイン内にあるすべてのルータは、既知の PIM RP アドレスを認識する必要があります。アドレスは、このコマンドを使用してスタティックに設定されます。

（注）　セキュリティ アプライアンス では、Auto-RP をサポートしません。**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

複数のグループにサービスを提供するように単一の RP を設定できます。アクセス リストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセス リストを指定しない場合、グループの RP は IP マルチキャスト グループの範囲（224.0.0.0/4）全体に適用されます。

（注）　セキュリティ アプライアンスは、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

例

次に、すべてのマルチキャスト グループに対して PIM RP アドレスを 10.0.0.1 に設定する例を示します。

```
hostname(config)# pim rp-address 10.0.0.1
```

関連コマンド

コマンド	説明
pim accept-register	PIM レジスタ メッセージをフィルタリングするように候補 RP を設定します。

pim spt-threshold infinity

常に共有ツリーを使用し、Shortest-Path Tree（SPT; 最短パス ツリー）スイッチオーバーを実行しないようにラスト ホップ ルータの動作を変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

構文の説明

group-list *acl*	（任意）送信元グループはアクセス リストによって制限されていることを示します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされません。

デフォルト

ラスト ホップ PIM ルータは、デフォルトで最短パスの送信元に切り替わります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

group-list キーワードを使用しない場合、このコマンドはすべてのマルチキャスト グループに適用されます。

例

次に、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するようにラスト ホップ PIM ルータを設定する例を示します。

```
hostname(config)# pim spt-threshold infinity
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

ping

他の IP アドレスがセキュリティ アプライアンスから認識できるかどうかを判断するには、特権 EXEC モードで **ping** コマンドを使用します。

ping [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

構文の説明

data *pattern*	（任意）16 進数による 16 ビットのデータ パターンを指定します。
host	ping の送信先ホストの IPv4 アドレス、IPv6 アドレス、または名前。名前は DNS 名、または **name** コマンドで割り当てた名前です。DNS 名の最大文字数は 128、**name** コマンドで作成した名前の最大文字数は 63 です。
if_name	（任意）*host* がアクセス可能なインターフェイス名を指定します。インターフェイス名は、**nameif** コマンドで設定します。指定しない場合、*host* は IP アドレスに解決され、宛先インターフェイスを決定するためにルーティング テーブルが参照されます。
repeat *count*	（任意）ping 要求を繰り返す回数を指定します。
size *bytes*	（任意）データグラム サイズをバイト数で指定します。
timeout *seconds*	（任意）ping 要求がタイムアウトするまでの秒数を指定します。
validate	（任意）応答データを検証するように指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	DNS 名のサポートが追加されました。

使用上のガイドライン

ping コマンドを使用すると、セキュリティ アプライアンスが接続可能かどうか、またはホストがネットワークで使用可能かどうかを判断できます。セキュリティ アプライアンスに接続できる場合は、**icmp permit any** *interface* コマンドが設定されていることを確認します。このコンフィギュレーションは、**ping** コマンドで生成されたメッセージに対して、セキュリティ アプライアンスが応答したり受け入れたりするために必要です。**ping** コマンドの出力は、応答が受け入れられたかどうかを示します。ホストが応答しない場合は、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

セキュリティ アプライアンス がネットワークに接続していて、トラフィックを送受信していることを確認するには、**show interface** コマンドを使用します。指定した *if_name* の名前は、ping の送信元アドレスとして使用されます。

内部ホストから外部ホストに対して ping を送信するには、次のいずれかの手順を実行します。

- エコー応答の場合は、ICMP **access-list** コマンドを使用します。たとえば、すべてのホストに対して ping アクセスを与えるには、**access-list acl_grp permit icmp any any** コマンドを使用し、**access-group** コマンドを使用してテストするインターフェイスに対して **access-list** コマンドをバインドします。
- **inspect icmp** コマンドを使用して ICMP インスペクション エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されるエコー要求に対して、エコー応答はセキュリティ アプライアンスを通過できます。

拡張された ping を実行することもできます。この場合、キーワードを一度に 1 行ずつ入力できます。

ホストやルータの間でセキュリティ アプライアンスを通過して ping を実行し、ping が成功しない場合、**capture** コマンドを使用して ping が成功するかどうかをモニタします。

セキュリティ アプライアンスの **ping** コマンドでは、インターフェイス名を必要としません。インターフェイス名を指定しない場合、指定したアドレスを探すためにセキュリティ アプライアンスはルーティング テーブルをチェックします。ICMP エコー要求の送信に使用されるインターフェイスを示すために、インターフェイス名を指定できます。

例

次に、他の IP アドレスがセキュリティ アプライアンスから認識できるかどうかを判断する例を示します。

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、DNS 名を使用してホストを指定する例を示します。

```
hostname# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、拡張された ping を使用する例を示します。

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

関連コマンド

コマンド	説明
capture	インターフェイスでパケットをキャプチャします。
icmp	インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。
show interface	VLAN コンフィギュレーションの情報を表示します。

police

QoS ポリシングをクラス マップに適用するには、クラス コンフィギュレーション モードで **police** コマンドを使用します。レート制限の要件を削除するには、このコマンドの **no** 形式を使用します。ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック フローが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、セキュリティ アプライアンスは超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

no police

構文の説明

conform-burst	適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。
conform-action	レートが *conform_burst* 値を下回ったときに実行するアクションを設定します。
conform-rate	このトラフィック フローのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。
drop	パケットをドロップします。
exceed-action	レートが *conform-rate* 値～ *conform-burst* 値の範囲にあるときに実行するアクションを設定します。
input	入力方向のトラフィック フローのポリシングをイネーブルにします。
output	出力方向のトラフィック フローのポリシングをイネーブルにします。
transmit	パケットを送信します。

デフォルト

デフォルトの動作や変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**input** オプションが追加されました。着信方向のトラフィックのポリシングがサポートされます。

使用上のガイドライン

ポリシングをイネーブルにするには、Modular Policy Framework を使用して次のように設定します。

1. **class-map**：ポリシングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **police**：クラス マップのポリシングをイネーブルにします。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

（注） **police** コマンドは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的にあわせるだけです。**conform-action** または **exceed-action** の指定は、存在する場合でも適用されません。

（注） conform-burst パラメータが省略された場合のデフォルト値は conform-rate のバイト数の 1/32 です（つまり、conform-rate が 100,000 の場合、conform-burst のデフォルト値は 100,000/32 = 3,125 です）。conform-rate の単位はビット / 秒で、conform-burst の単位はバイト数です。

セキュリティ アプライアンスで必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能をセキュリティ アプライアンスに設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

  同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定はセキュリティ アプライアンスでは制限されていません。

確立済みの VPN クライアント /LAN-to-LAN または非トンネル トラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリア（つまりドロップ）して再確立する必要があります。

例

次に、出力方向の **police** コマンドの例を示します。このコマンドは、適合レートを 100,000 ビット / 秒、バースト値を 20,000 バイトに設定し、バースト レートを超えたトラフィックはドロップされるように指定します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class-map firstclass
hostname(config-cmap)# class localclass
hostname(config-pmap-c)# police output 100000 20000 exceed-action drop
hostname(config-cmap-c)# class class-default
hostname(config-pmap-c)#
```

次に、内部 Web サーバを宛先とするトラフィックにレート制限を実行する例を示します。

```
hostname# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
```

```
hostname# class-map http_traffic
hostname(config-cmap)# match access-list http_traffic
hostname(config-cmap)# policy-map outside_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# police input 56000
hostname(config-pmap-c)# service-policy outside_policy interface outside
hostname(config)#
```

関連コマンド

class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

policy

CRL の取得元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

policy {**static** | **cdp** | **both**}

構文の説明

both	CRL 配布ポイントを使用した CRL の取得に失敗した場合は、スタティック CDP を最大 5 つ使用して再試行します。
cdp	チェック対象の証明書内に埋め込まれている CDP 拡張を使用します。この場合、セキュリティ アプライアンスは検証対象の証明書の CDP 拡張から最大 5 つの CRL 配布ポイントを取得します。さらに必要に応じて、設定されたデフォルト値を使用して情報を増強します。セキュリティ アプライアンスがプライマリ CDP を使用して CRL を取得するのに失敗した場合は、リストで次に使用可能な CDP を使用して再試行します。これは、セキュリティ アプライアンスが CRL を取得するかリストの最後に到達するまで、繰り返されます。
static	最大で 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドを使用して LDAP または HTTP URL も指定します。

デフォルト

デフォルトの設定は **cdp** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、チェック対象の証明書内にある CRL 配布ポイント拡張を使用して CRL 取得を行うように設定し、失敗した場合はスタティック CDP を使用する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
url	CRL 取得用のスタティック URL のリストを作成および維持します。

policy-map

モジュラ ポリシー フレームワーク を使用する場合、レイヤ 3/4 のクラスマップ（**class-map** または **class-map type management** コマンド）を使用してトラフィックにアクションを割り当てるには、グローバル コンフィギュレーション モードで **policy-map** コマンド（**type** キーワードの指定なし）を使用します。レイヤ 3/4 ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map *name*

no policy-map *name*

構文の説明

name	このポリシー マップの名前を最大 40 文字で指定します。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

ポリシー マップの最大数は 64 です。レイヤ 3/4 ポリシー マップ内にある複数のレイヤ 3/4 クラス マップを特定でき（**class** コマンドを参照）、1 つ以上の機能タイプから各クラス マップへ複数のアクションを割り当てることができます。

パケットは、各機能タイプのポリシー マップで、1 つのクラス マップにだけ一致します。パケットが機能タイプのクラス マップと一致する場合、セキュリティ アプライアンスはその機能タイプについて後続のクラス マップと照合しません。ただし、パケットが別の機能タイプについて後続のクラス マップと一致する場合、セキュリティ アプライアンスでは後続のクラス マップについてもアクションを適

用します。たとえば、パケットが接続制限についてのクラス マップと一致し、さらにアプリケーション インスペクションについてのクラス マップとも一致する場合は、両方のクラス マップ アクションが適用されます。パケットがアプリケーション インスペクションについてのクラス マップと一致し、さらにアプリケーション インスペクションについての別のクラス マップとも一致する場合、2 番めのクラス マップ アクションは適用されません。

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

（注） グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS のように単方向に適用される機能では、ポリシー マップの適用先インターフェイスから出るトラフィックのみが影響を受けます。各機能の方向については、表 22-1 を参照してください。

表 22-1　機能の方向

機能	単一インターフェイスでの方向	グローバルでの方向
TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化	双方向	入力
CSC	双方向	入力
アプリケーション インスペクション	双方向	入力
IPS	双方向	入力
QoS ポリシング	Egress	Egress
QoS プライオリティ キュー	Egress	Egress

ポリシー マップの各種のアクションが実行される順序は、ポリシー マップ中に出現する順序とは無関係です。アクションは次の順序で実行されます。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化

（注） セキュリティ アプライアンスがプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

- CSC
- アプリケーション インスペクション
- IPS
- QoS ポリシング
- QoS プライオリティ キュー

インターフェイスあたりに割り当てられるポリシー マップは 1 つだけですが、同じポリシー マップを複数のインターフェイスに割り当てることができます。

コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用する、デフォルトのレイヤ 3/4 ポリシー マップが含まれています。これは **global_policy** と呼ばれ、デフォルトのインスペクション トラフィックでインスペクションを実行します。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルトのポリシー マップ コンフィギュレーションには、次のコマンドが含まれます。

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

例

接続ポリシーの **policy-map** コマンドの例を次に示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
```

```
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、セキュリティ アプライアンスはこの照合を行いません。

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ポリシー マップが **service-policy** コマンドで使用されている場合、そのポリシー マップは削除されません。
class-map	トラフィック クラス マップを定義します。
service-policy	ポリシー マップをインターフェイスに割り当てるか、またはすべてのインターフェイスにグローバルに割り当てます。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

policy-map type inspect

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map type inspect** コマンドを使用して、アプリケーション トラフィック検査のための特別なアクションを定義します。インスペクション ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

構文の説明

application	対象とするアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **sip** • **skinny** • **snmp**
policy_map_name	このポリシー マップの名前を最大 40 文字で指定します。「_internal」または「_default」で始まる名前は予約されており、使用できません。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で、**inspect** コマンドを使用してインスペクション エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシー マップで定義されているアクションを、オプションでイネーブルにすることもできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、ポリシー マップ コンフィギュレーション モードで入力するコマンドのうち、次の 1 つ以上のコマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。

- **match** コマンド：**match** コマンドをインスペクション ポリシー マップで直接定義して、アプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合できます。次に、一致コンフィギュレーション モードで **drop**、**reset**、**log** などのアクションをイネーブルにします。**match** コマンドを使用できるかどうかは、アプリケーションによって異なります。
- **class** コマンド：このコマンドは、ポリシー マップ内のインスペクション クラス マップを特定します（インスペクション クラス マップの作成については、**class-map type inspect** コマンドを参照してください）。インスペクション クラス マップには、**match** コマンドが含まれます。このコマンドは、ポリシー マップ内のアクションをイネーブルにするアプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合します。クラス マップを作成することと、インスペクション ポリシー マップ内で **match** コマンドを直接使用することの違いは、複数の照合結果をグループ化できることと、クラス マップを再使用できることです。
- **parameters** コマンド：パラメータは、インスペクション エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。

一部の **match** コマンドでは、パケット内のテキストと一致させるために正規表現を指定できます。**regex** コマンドおよび **class-map type regex** コマンド（複数の正規表現をグループ化）を参照してください。

デフォルトのインスペクション ポリシー マップ コンフィギュレーションには、次のコマンドが組み込まれています。このコンフィギュレーションでは、DNS パケットの最大メッセージ長を 512 バイトに設定しています。

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、セキュリティ アプライアンス がアクションを適用する順序は、ポリシー マップにアクションが追加された順序ではなく、セキュリティ アプライアンスの内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
hostname(config-pmap)# match request header host length gt 100
hostname(config-pmap-c)# reset
hostname(config-pmap-c)# match request method get
hostname(config-pmap-c)# log
```

アクションがパケットをドロップすると、それ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドが一致することはありません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます 同じ **match** コマンドに対して **reset**（または **drop-connection** など）と **log** アクションの両方を設定できます。この場合、特定の match でリセットされるまでパケットはログに記録されます。

パケットが、同じ複数の **match** コマンドまたは **class** コマンドと照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
hostname(config-pmap)# match request header length gt 100
hostname(config-pmap-c)# log
hostname(config-pmap-c)# match request header length gt 1000
hostname(config-pmap-c)# reset
```

クラス マップは、そのクラス マップ内で重要度が最低の **match** コマンド（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは **match** コマンドと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の **match** コマンドがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度のコマンドが異なる場合は、最高重要度の **match** コマンドを持つクラス マップが最初に照合されます。

例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
```

```
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
parameters	インスペクション ポリシー マップのパラメータ コンフィギュレーション モードを開始します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

policy-server-secret

SiteMinder SSO サーバへの認証要求を暗号化するために使用する秘密キーを設定するには、webvpn sso siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用します。秘密キーを削除するには、このコマンドの **no** 形式を使用します。

policy-server-secret *secret-key*

no policy-server-secret

（注） このコマンドは、SiteMinder SSO 認証で必要です。

構文の説明

secret-key	認証通信を暗号化するために秘密キーとして使用されるストリング。文字の最小数や最大数の制限はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-siteminder コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。まず **sso-server** コマンドを使用して SSO サーバを作成します。SiteMinder SSO サーバの場合、**policy-server-secret** コマンドによってセキュリティ アプライアンスと SSO サーバの間の認証通信を保護します。

コマンド引数 *secret-key* は、パスワードと同様に作成、保存、および設定が可能です。このコマンド引数は、**policy-server-secret** コマンドを使用してセキュリティ アプライアンスで設定され、Cisco Java プラグイン認証方式を使用して SiteMinder Policy Server で設定されます。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

例

次に、config-webvpn-sso-siteminder モードで、引数としてランダムなストリングを使用して、SiteMinder SSO サーバ認証通信の秘密キーを作成する例を示します。

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
```

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

polltime interface

Active/Active フェールオーバー コンフィギュレーションのデータ インターフェイス ポーリング タイムおよびホールド タイムを指定するには、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

polltime interface [**msec**] *time* [**holdtime** *time*]

no polltime interface [**msec**] *time* [**holdtime** *time*]

構文の説明

holdtime *time*	（任意）データ インターフェイスがピア インターフェイスから hello メッセージを受信する必要のある時間を設定します。この時間の経過後、ピア インターフェイスが障害状態であると宣言されます。有効な値は 5 ～ 75 秒です。
interface *time*	データ インターフェイスのポーリング期間を指定します。有効な値は、3 ～ 15 秒です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。

デフォルト

ポーリングの *time* は 5 秒です。

holdtime *time* は、ポーリングの *time* の 5 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは、任意の **holdtime** *time* 値とポーリング タイムをミリ秒で指定する機能を含めるように変更されました。

使用上のガイドライン

指定されたフェールオーバー グループと関連付けられたインターフェイスから hello パケットが送信される頻度を変更するには、**polltime interface** コマンドを使用します。このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。Active/Standby フェールオーバー コンフィギュレーションで **failover polltime interface** コマンドを使用します。

ポーリング タイムの 5 倍よりも短い **holdtime** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ホールド タイムの半分が経過したときに、インターフェイスで hello パケットが受信されていない場合は、インターフェイスのテストが開始されます。

failover polltime unit コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。フェールオーバー グループ 1 のデータ インターフェイスのインターフェイス ポーリング時間を 500 ミリ秒に設定し、保持時間を 5 秒に設定します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover polltime	装置のフェールオーバー ポーリング期間とホールド タイムを指定します。
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。

pop3s

POP3S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンド モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

POP3 は、インターネット サーバが電子メールを受信して保持するために使用するクライアント / サーバ プロトコルです。ユーザ（またはクライアント電子メール レシーバ）は、定期的にメールボックスをチェックして、メールがある場合はそれをダウンロードします。この標準プロトコルは、ほとんどの著名な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

pop3s

no pop3

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、POP3S コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。

port

電子メール プロキシで受信に使用されるポートを指定するには、適切な電子メール プロキシ コマンド モードで **port** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

port {*portnum*}

no port

構文の説明

portnum	電子メール プロキシで使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

デフォルト

電子メール プロキシのデフォルト ポートは次のとおりです。

電子メール プロキシ	デフォルト ポート
IMAP4S	993
POP3S	995
SMTPS	988

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

例

次に、IMAP4S 電子メール プロキシ用にポート 1066 を設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

port-forward

クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートからアクセスできるアプリケーション セットを設定するには、webvpn コンフィギュレーション モードで **port-forward** コマンドを使用します。

port-forward {*list_name local_port remote_server remote_port description*}

複数アプリケーションへのアクセスを設定するには、アプリケーションごとに同じ *list_name* を 1 回ずつ、複数回指定してこのコマンドを使用します。

リストから設定済みアプリケーションを削除するには、**no port-forward** *list_name local_port* コマンドを使用します（*remote_server* および *remote_port* パラメータを指定する必要はありません）。

no port-forward *listname localport*

設定済みのリスト全体を削除するには、**no port-forward** *list_name* コマンドを使用します。

no port-forward *list_name*

構文の説明

description	エンド ユーザのポート フォワーディング Java アプレット画面に表示されるアプリケーション名または短い説明を指定します。最大 64 文字です。
list_name	クライアントレス SSL VPN セッションのユーザがアクセスできる一連のアプリケーション（転送先 TCP ポート）をグループ化します。最大 64 文字です。
local_port	アプリケーションの TCP トラフィックを受信するローカル ポートを指定します。ローカル ポート番号は *list_name* あたり 1 回のみ使用できます。1 ～ 65535 の範囲のポート番号を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。
remote_port	リモート サーバでこのアプリケーション用に接続するポートを指定します。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。
remote_server	アプリケーションのリモート サーバの DNS 名または IP アドレスを指定します。これには DNS 名を使用することを推奨します。IP アドレスを入力する場合は、IPv4 形式か IPv6 形式で入力できます。

デフォルト

デフォルトのポート フォワーディング リストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(2)	コマンド モードが webvpn に変更されました。

使用上のガイドライン

セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。クライアントレス SSL VPN セッションを介してアプリケーション アクセスを提供する、ポート フォワーディングとスマート トンネル機能のいずれも、MAPI をサポートしていません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。

例

次の表に、サンプル アプリケーションで使用する値を示します。

アプリケーション	Local Port	サーバ DNS 名	Remote Port	説明
IMAP4S 電子メール	20143	IMAP4Sserver	143	メール取得
SMTPS 電子メール	20025	SMTPSserver	25	メール送信
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

次に、これらのアプリケーションへのアクセスを提供する *SalesGroupPorts* という名前のポート フォワーディング リストを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

関連コマンド

コマンド	説明
port-forward auto-start	このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ユーザがクライアントレス SSL VPN セッションにログインするときに、ポート フォワーディングを自動的に開始して、指定したポート フォワーディング リストを割り当てます。
port-forward enable	このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ユーザがログインするときに、指定したポート フォワーディング リストを割り当てますが、ポート フォワーディングはユーザが手動で開始する必要があります。開始するには、クライアントレス SSL VPN ポータル ページで [Application Access] > [Start Applications] ボタンを使用します。
port-forward disable	このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ポート フォワーディングをオフにします。

port-forward-name

特定のユーザ ポリシーやグループ ポリシーのエンド ユーザに対して TCP ポート フォワーディングを特定する表示名を設定するには、webvpn モードで **port-forward-name** コマンドを使用します。このモードは、グループ ポリシー モードまたはユーザ名モードから開始します。表示名（**port-forward-name none** コマンドを使用して作成されたヌル値を含む）を削除するには、このコマンドの no 形式を使用します。**no** オプションを使用するとデフォルト名「Application Access」に戻ります。表示名を使用しないようにするには、**port-forward none** コマンドを使用します。

port-forward-name {**value** *name* | **none**}

no port-forward-name

構文の説明

none	表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値は継承しません。
value *name*	エンド ユーザにポート フォワーディングを説明します。最大 255 文字です。

デフォルト

デフォルト名は「Application Access」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーに対して「Remote Access TCP Applications」という名前を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

port-object

サービス オブジェクト グループにポート オブジェクトを追加するには、サービス コンフィギュレーション モードで **port-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

構文の説明

begin_service	サービスの範囲の開始値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 とする必要があります。
end_service	サービスの範囲の終了値である TCP または UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 とする必要があります。
eq service	サービス オブジェクトの TCP または UDP ポートの 10 進数または名前を指定します。
range	ポートの範囲（両端を含む）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
サービス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

port-object コマンドは、**object-group** コマンドとともに使用して、サービス コンフィギュレーション モードで特定サービス（ポート）またはサービス（ポート）の範囲であるオブジェクトを定義します。

TCP または UDP サービスの名前を指定する場合は、サポートされる TCP や UDP のいずれかの名前で、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、プロトコル タイプが tcp、udp、および tcp-udp の場合、名前はそれぞれ有効な TCP サービス名、有効な UDP サービス名、または有効な TCP および UDP サービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコル タイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

TCP	UDP	TCP および UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

例

次に、新規ポート（サービス）オブジェクト グループを作成するために、サービス コンフィギュレーション モードで **port-object** コマンドを使用する例を示します。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

post-max-size

オブジェクトのポストが許可される最大サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **post-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

post-max-size <*size*>

no post-max-size

構文の説明

size	ポストするオブジェクトに許可される最大サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

サイズを 0 に設定すると、オブジェクトのポストが実質的に禁止されます。

例

次に、ポストするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# post-max-size 1500
```

関連コマンド

コマンド	説明
download-max-size	ダウンロードするオブジェクトの最大サイズを指定します。
upload-max-size	アップロードするオブジェクトの最大サイズを指定します。

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

pppoe client route distance

PPPoE を介して学習したルートのアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pppoe client route distance *distance*

no pppoe client route distance *distance*

構文の説明

distance	PPPoE を介して学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

デフォルト

PPPoE を介して学習したルートには、デフォルトで 1 のアドミニストレーティブ ディスタンスが割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルートが PPPoE から学習されたときにのみ、**pppoe client route distance** コマンドがチェックされます。ルートが PPPoE から学習された後で **pppoe client route distance** コマンドを入力しても、指定したアドミニストレーティブ ディスタンスは既存の学習済みルートに影響しません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。複数のインターフェイスでの PPPoE クライアントのイネーブル化は、オブジェクト トラッキングでのみサポートされています。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client route track

PPPoE クライアントを設定して、追加されたルートを指定されたトラッキング済みオブジェクト番号に関連付けるには、インターフェイス コンフィギュレーション モードで **pppoe client route track** コマンドを使用します。PPPoE ルート トラッキングを削除するには、このコマンドの **no** 形式を使用します。

pppoe client route track *number*

no pppoe client route track

構文の説明

number	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルートが PPPoE から学習されたときにのみ、**pppoe client route track** コマンドがチェックされます。ルートが PPPoE から学習された後に **pppoe client route track** コマンドを入力した場合、既存の学習されたルートはトラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client secondary

PPPoE クライアントをトラッキング済みオブジェクトのクライアントとして登録し、トラッキング状態に基づいて起動または終了するように設定するには、インターフェイス コンフィギュレーション モードで **pppoe client secondary** コマンドを使用します。クライアントの登録を削除するには、このコマンドの **no** 形式を使用します。

pppoe client secondary track *number*

no pppoe client secondary track

構文の説明

number	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PPPoE セッションが開始されたときにのみ、**pppoe client secondary** コマンドがチェックされます。ルートが PPPoE から学習された後に **pppoe client route track** コマンドを入力した場合､既存の学習されたルートはトラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。

pre-fill-username

認証と認可で使用するクライアント証明書からユーザ名を抽出できるようにするには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

pre-fill-username {**ssl-client** | **clientless**}

no pre-fill-username

構文の説明

ssl-client	この機能を AnyConnect VPN クライアント接続でイネーブルにします。
clientless	この機能をクライアントレス接続でイネーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

pre-fill-username コマンドを使用すると、ユーザ名 / パスワードによる認証と認可のユーザ名として、**username-from-certificate** コマンドで指定した証明書のフィールドから抽出したユーザ名を使用できます。証明書機能からこの事前充填ユーザ名を使用するには、両方のコマンドを設定する必要があります。

この機能をイネーブルにするには、トンネル グループ一般属性モードで **usesrname-from-certificate** コマンドを設定する必要もあります。

（注） リリース 8.0.4 では、ユーザ名は事前に入力されません。ユーザ名フィールド内の送信されたデータは無視されます。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、SSL VPN クライアントの認証または認可クエリーの名前をデジタル証明書から取得する必要があることを指定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp webvpn-attributes
```

```
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

preempt

ユニットのプライオリティが高い場合にそのユニットをブート時にアクティブにするには、フェールオーバー グループ コンフィギュレーション モードで **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

preempt [*delay*]

no preempt [*delay*]

構文の説明

seconds	ピアがプリエンプション処理されるまでの待機時間（秒数）。有効な値は、1 ～ 1200 秒です。

デフォルト

デフォルトでは遅延はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てると、両方のユニットが（ユニットのポーリング期間内で）同時にブートしたときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。しかし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバー グループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバー グループが自動的にアクティブになります。

（注） ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どちらのフェールオーバー グループも **preempt** コマンドで待機時間が 100 秒に設定されているため、グループは、ユニットが使用可能になった 100 秒後に自動的にその優先ユニットでアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
primary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、プライマリ ユニットを指定します。
secondary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、セカンダリ ユニットを指定します。

prefix-list

ABR のタイプ 3 LSA フィルタリングのプレフィックス リストにエントリを作成するには、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックス リストのエントリを削除するには、このコマンドの **no** 形式を使用します。

prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

構文の説明

/	*network* 値と *len* 値との間に必要な区切り文字。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（任意）照会されるプレフィックスの最小の長さを指定します。*min_value* 引数の値は、*len* 引数の値よりも大きく、*max_value* 引数が存在する場合はそれ以下である必要があります。
le *max_value*	（任意）照会されるプレフィックスの最大の長さを指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合はその値以上、*min_value* 引数が存在しない場合は *len* 引数よりも大きい値にする必要があります。
len	ネットワーク マスクの長さ。有効な値は、0 ～ 32 です。
network	ネットワーク アドレス。
permit	一致した条件へのアクセスを許可します。
prefix-list-name	プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。
seq *seq_num*	（任意）作成するプレフィックス リストに指定されたシーケンス番号を適用します。

デフォルト

シーケンス番号を指定しない場合、プレフィックス リストの先頭エントリにはシーケンス番号 5 が割り当てられ、その後のエントリのシーケンス番号は 5 ずつ増えていきます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

prefix-list コマンドは、ABR のタイプ 3 LSA フィルタリング コマンドです。ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスのみがエリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。セキュリティ アプライアンスでは、プレフィックス リストの先頭、つまりシーケンス番号が最も小さいエントリから検索を開始します。一致が見つかると、セキュリティ アプライアンスはリストの残りの部分を調べません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。自動生成されるシーケンス番号を抑制するには、**no prefix-list sequence-number** コマンドを使用します。シーケンス番号は、5 ずつ増分されます。プレフィックス リストで生成される最初のシーケンス番号は 5 です。そのリストの次のエントリにはシーケンス番号 10 が設定され、以降も同様に設定されます。あるエントリに値を指定し、その後のエントリに値を指定しない場合、生成されるシーケンス番号は指定された値から 5 ずつ増分されます。たとえば、プレフィックス リストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら 2 つエントリに対して自動的に生成されるシーケンス番号は、8 および 13 となります。

ge キーワードおよび **le** キーワードを使用して、*network*/*len* 引数よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。**ge** キーワードも **le** キーワードも指定されていないときは、完全一致であると見なされます。**ge** キーワードのみが指定されている場合の範囲は、*min_value* ～ 32 です。**le** キーワードのみが指定されている場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たす必要があります。

len < *min_value* <= *max_value* <= 32

プレフィックス リストから特定のエントリを削除するには、このコマンドの **no** 形式を使用します。プレフィックス リストを削除するには、**clear configure prefix-list** コマンドを使用します。**clear configure prefix-list** コマンドを使用すると、関連する **prefix-list description** コマンドがある場合は、それもコンフィギュレーションから削除されます。

例

次に、デフォルト ルート 0.0.0.0/0 を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

次に、プレフィックス 10.0.0.0/8 を許可する例を示します。

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

次に、プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する例を示します。

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次に、プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次に、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する例を示します。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次に、すべてのアドレス空間で 25 ビットよりも大きいマスク長を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次に、プレフィックス 10/8 のすべてのルートを拒否する例を示します。

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次に、プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する例を示します。

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次に、プレフィックス 0/0 のすべてのルートを許可する例を示します。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list description	プレフィックス リストの説明を入力できます。
prefix-list sequence-number	プレフィックス リストのシーケンス番号付けをイネーブルにします。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list description

プレフィックス リストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックス リストの説明を削除するには、このコマンドの **no** 形式を使用します。

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

構文の説明

prefix-list-name	プレフィックス リストの名前。
text	プレフィックス リストの説明テキスト。最大 80 文字を入力できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

prefix-list コマンドおよび **prefix-list description** コマンドは、特定のプレフィックス リスト名に対して、任意の順序で入力できます。プレフィックス リストの説明を入力する前に、プレフィックス リストを作成する必要はありません。**prefix-list description** コマンドは、コマンドを入力する順序に関係なく、コンフィギュレーションで関連するプレフィックス リストの前の行に必ず記述されます。

すでに説明の設定されたプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、新しい説明によって元の説明が置き換えられます。

このコマンドの **no** 形式を使用するときは、テキスト説明を入力する必要はありません。

例

次に、MyPrefixList という名前のプレフィックス リストの説明を追加する例を示します。**show running-config prefix-list** コマンドは、プレフィックス リストの説明が実行コンフィギュレーションに追加された場合でも、プレフィックス リスト自体は設定されていないことを示します。

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィックス リストのシーケンス番号付けをイネーブルにするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィックス リストのシーケンス番号付けをディセーブルにするには、このコマンドの **no** 形式を使用します。

prefix-list sequence-number

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式がコンフィギュレーション内にある場合、シーケンス番号（手動設定したものを含む）はコンフィギュレーション内の **prefix-list** コマンドから削除されます。プレフィックス リストの新しいエントリにシーケンス番号は割り当てられません。

プレフィックス リストのシーケンス番号付けがイネーブルの場合、デフォルトの番号付け方式（5 で始まり、番号が 5 ずつ増分される）を使用して、プレフィックス リストのすべてのエントリにシーケンス番号が割り当てられます。番号付けがディセーブルになる前に、シーケンス番号がプレフィックス リストのエントリに手動で割り当てられた場合、手動で割り当てられた番号が復元されます。自動番号付けがディセーブルのときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、これらのシーケンス番号は表示されません。

例

次に、プレフィックス リストのシーケンス番号付けをディセーブルにする例を示します。

```
hostname(config)# no prefix-list sequence-number
```

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

pre-shared-key

事前共有キーを指定して、事前共有キーに基づく IKE 接続をサポートするには、トンネル グループ IPSec 属性コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pre-shared-key *key*

no pre-shared-key

構文の説明

key	1 ～ 128 文字の英数字キーを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

例

次に、設定 IPSec コンフィギュレーション モードで、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE 接続をサポートするように事前共有キー XYZX を指定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

primary

プライマリ ユニットにフェールオーバー グループで高いプライオリティを指定するには、フェールオーバー グループ コンフィギュレーション モードで **primary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

primary

no primary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てると、両方のユニットが（ユニットのポーリング期間内で）同時にブートしたときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。あるユニットがもう一方のユニットよりも先にブートした場合、両方のフェールオーバー グループがそのユニットでアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
```

```
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。
secondary	セカンダリ ユニットにプライマリ ユニットよりも高いプライオリティを指定します。

priority

QoS プライオリティ キューイングをイネーブルにするには、クラス コンフィギュレーション モードで **priority** コマンドを使用します。Voice over IP（VoIP）のように遅延を許容できないクリティカルなトラフィックでは、常に最低レートで送信されるように Low Latency Queueing（LLQ; 低遅延キューイング）のトラフィックを特定できます。プライオリティの要件を削除するには、このコマンドの **no** 形式を使用します。

priority

no priority

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

セキュリティ アプライアンスは、次の 2 タイプのプライオリティ キューイングをサポートしています。

- 標準プライオリティ キューイング：標準プライオリティ キューイングではインターフェイスで LLQ プライオリティ キューを使用しますが（**priority-queue** コマンドを参照）、他のすべてのトラフィックは「ベスト エフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。
- 階層型プライオリティ キューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キュー（**shape** コマンド）がイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。階層型プライオリティ キューイングについては、次のガイドラインを参照してください。

- プライオリティ パケットは常にシェープ キューの先頭に格納されるので、常に他の非プライオリティ キュー パケットよりも前に送信されます。
- プライオリティ トラフィックの平均レートがシェープ レートを超えない限り、プライオリティ パケットがシェープ キューからドロップされることはありません。
- IPSec-encrypted パケットの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。
- プライオリティ トラフィック分類では、IPSec-over-TCP はサポートされません。

Modular Policy Framework を使用した QoS の設定

プライオリティ キューイングをイネーブルにするには、Modular Policy Framework を使用します。標準プライオリティ キューイングまたは階層型プライオリティ キューイングを使用できます。

標準プライオリティ キューイングの場合は、次の作業を実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

階層型プライオリティ キューイングの場合は、次の作業を実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。
3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**：トラフィック シェーピングをクラス マップに適用します。
   c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、ポリシー マップ モードでの **priority** コマンドの例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

関連コマンド

class	トラフィック分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

priority（vpn ロード バランシング）

仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定するには、VPN ロード バランシング モードで **priority** コマンドを使用します。デフォルトのプライオリティ指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*

no priority

構文の説明

priority	このデバイスに割り当てるプライオリティ（1 ～ 10 の範囲）。

デフォルト

デフォルトのプライオリティは、デバイスのモデル番号によって異なります。

モデル番号	デフォルトのプライオリティ
5520	5
5540	7

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング	—	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始する必要があります。

このコマンドは、仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定します。

プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。

プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の 1 つとして、マスター選出プロセスで使用されます。マスター選出プロセスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

プライオリティ指定をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

例

次に、現在のデバイスのプライオリティを 9 に設定する **priority** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

priority-queue

priority コマンドで使用するインターフェイスで標準プライオリティ キューを作成するには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。キューを削除するには、このコマンドの **no** 形式を使用します。

priority-queue *interface-name*

no priority queue *interface-name*

構文の説明

interface-name	プライオリティ キューをイネーブルにする物理インターフェイスの名前を指定します。ASA 5505 の場合は、VLAN インターフェイスの名前を指定します。

デフォルト

デフォルトでは、プライオリティ キューイングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

セキュリティ アプライアンスは、次の 2 タイプのプライオリティ キューイングをサポートしています。

- 標準プライオリティ キューイング：標準プライオリティ キューイングでは、インターフェイスで **priority-queue** コマンドを使用して作成する LLQ プライオリティ キューを使用しますが、他のすべてのトラフィックは「ベスト エフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになるのを回避するために、キューのバッファ サイズを増やすことができます（**queue-limit** コマンド）。また、送信キュー内に受け入れ可能な最大パケット数を微調整することもできます（**tx-ring-limit** コマンド）。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

- 階層型プライオリティ キューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キューがイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。

ASA モデル 5505（のみ）では、1 つのインターフェイスにプライオリティ キューを設定すると、他のすべてのインターフェイスで同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけが、すべてのインターフェイスに存在することになります。さらに、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスからも削除されます。

この問題を回避するには、**priority-queue** コマンドを 1 つのインターフェイスにのみ設定します。**queue-limit** コマンドと **tx-ring-limit** コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

関連コマンド

コマンド	説明
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
clear configure priority-queue	現在のプライオリティ キュー コンフィギュレーションを削除します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティ キュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。

privilege

コマンド認可（ローカル、RADIUS、および LDAP（マッピング）のみ）で使用するコマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。コンフィギュレーションを拒否するには、このコマンドの **no** 形式を使用します。

privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

no privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

構文の説明

clear	（任意）コマンドの clear 形式に対してのみ特権を設定します。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。
command *command*	設定するコマンドを指定します。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。 また、サブコマンドの特権レベルは main コマンドと別に設定することもできません。たとえば、**context** コマンドは設定できますが、**allocate-interface** コマンドは **context** コマンドから設定を継承するため、設定できません。
configure	（任意）コマンドの configure 形式に対してのみ特権を設定します。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。
level *level*	特権レベルを指定します。有効な値は、0 ～ 15 です。特権レベルの番号が小さいと、特権レベルが低くなります。
mode enable	（任意）1 つのコマンドをコンフィギュレーション モードだけでなくユーザ EXEC モードおよび特権 EXEC モードで入力することができ、このコマンドが各モードで異なるアクションを実行する場合は、これらのモードに別々に特権レベルを設定できます。**mode enable** キーワードでは、ユーザ EXEC モードと特権 EXEC モードの両方を指定します。
mode configure	（任意）1 つのコマンドをコンフィギュレーション モードだけでなくユーザ EXEC モードおよび特権 EXEC モードで入力することができ、このコマンドが各モードで異なるアクションを実行する場合は、これらのモードに別々に特権レベルを設定できます。**mode configure** キーワードは、**configure terminal** コマンドを使用してアクセスするコンフィギュレーション モードを指定します。
show	（任意）コマンドの show 形式に対してのみ特権を設定します。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。

デフォルト

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは、レベル 15 です。

- **show checksum**
- **show curpriv**

- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示するには、**show running-config all privilege all** コマンドを参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	Cisco VSA CVPN3000-Privilege-Level を使用する RADIUS ユーザのサポートが追加されました。**ldap map-attributes** コマンドを使用して LDAP 属性を CVPN3000-Privilege-Level にマッピングすると、LDAP ユーザがサポートされます。

使用上のガイドライン

privilege コマンドを使用すると、**aaa authorization command LOCAL** コマンドを設定するときに、セキュリティ アプライアンス コマンドの特権レベルを設定できます。このコマンドで **LOCAL** キーワードを使用する場合でも、このキーワードによってローカル、RADIUS、および LDAP（マッピング）認可がイネーブルになります。

例

たとえば、**filter** コマンドには次の形式があります。

- **filter**（**configure** オプションで表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、それぞれの形式を別々に設定するには、次のように指定します。

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

また、すべてのフィルタ コマンドを同じレベルに設定できます。

```
hostname(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

次に、追加のコマンド **configure** コマンドの例を示します。このコマンドでは **mode** キーワードを使用します。

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

（注）　この最後の行は、**configure terminal** コマンドで使用します。

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

prompt

CLI プロンプトをカスタマイズするには、グローバル コンフィギュレーション モードで **prompt** コマンドを使用します。デフォルトのプロンプトに戻すには、このコマンドの **no** 形式を使用します。

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]}

no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]

構文の説明

context	（マルチ モードのみ）現在のコンテキストを表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。
state	装置のトラフィック通過状態を表示します。state キーワードに対して、次の値が表示されます。 • [act] : フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • stby : フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove] : フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover] : フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。

デフォルト

デフォルトのプロンプトはホスト名です。マルチ コンテキスト モードでは、ホスト名の後に現在のコンテキスト名が続きます（*hostname*/*context*）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

プロンプトに情報を追加できるため、複数のモジュールがある場合に、どのセキュリティ アプライアンスにログインしているかを一目で確認できます。この機能は、フェールオーバー時に、両方のセキュリティ アプライアンスに同じホスト名が設定されている場合に便利です。

例

次に、プロンプトで使用可能なすべての要素を表示する例を示します。

```
hostname(config)# prompt hostname context priority state
```

プロンプトが次のストリングに変化します。

```
hostname/admin/pri/act(config)#
```

関連コマンド

コマンド	説明
clear configure prompt	設定したプロンプトをクリアします。
show running-config prompt	設定したプロンプトを表示します。

protocol-enforcement

ドメイン名、ラベル長、形式チェック（圧縮およびループ ポインタのチェックを含む）をイネーブルにするには、パラメータ コンフィギュレーション モードで **protocol-enforcement** コマンドを使用します。プロトコルの強制をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol-enforcement

no protocol-enforcement

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

プロトコルの強制は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no protocol-enforcement** を明示的に記述する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

状況によっては、コマンドがディセーブルであっても、プロトコルの強制が実行されます。これは、DNS リソース レコードの分類、NAT、TSIG チェックなど、他の目的で DNS リソース レコードの解析が必要なときに発生します。

例

次に、DNS インスペクション ポリシー マップ内でプロトコルの強制をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

protocol http

CRL を取得するための許可された配布ポイント プロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

protocol http

no protocol http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は、HTTP を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Ca-CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する場合は、HTTP ルールをパブリック インターフェイス フィルタに適用してください。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして HTTP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイント プロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol ldap

no protocol ldap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は、LDAP を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして LDAP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol http	CRL の取得方法として HTTP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol scep

CRL を取得するための配布ポイント プロトコルとして SCEP を指定するには、crl コンフィギュレーション モードで **protocol scep** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol scep

no protocol scep

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は、SCEP を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして SCEP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol http	CRL の取得方法として HTTP を指定します。
protocol ldap	CRL の取得方法として LDAP を指定します。

protocol-object

プロトコル オブジェクト グループにプロトコル オブジェクトを追加するには、プロトコル コンフィギュレーション モードで **protocol-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

protocol-object *protocol*

no protocol-object *protocol*

構文の説明

protocol	プロトコルの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プロトコル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

protocol-object コマンドは、**object-group** コマンドとともに使用して、プロトコル コンフィギュレーション モードでプロトコル オブジェクトを定義します。

IP プロトコルの名前や番号は、*protocol* 引数を使用して指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

例

次に、プロトコル オブジェクトを定義する例を示します。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

protocol-violation

HTTP および NetBIOS インスペクションでプロトコル違反が発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **protocol-violation** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol-violation action [**drop** [**log**] | **log**]

no protocol-violation action [**drop** [**log**] | **log**]

構文の説明

drop	プロトコルに準拠しないパケットをドロップすることを指定します。
log	プロトコル違反をログに記録することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、HTTP または NetBIOS ポリシー マップで設定できます。HTTP または NetBIOS パーサーが HTTP または NetBIOS メッセージの最初の数バイトで有効なメッセージを検出できない場合、syslog が発行されます。たとえば、チャンク エンコーディングの形式が不正であるためにメッセージを解析できない場合に、このような状況が発生します。

例

次に、ポリシー マップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation action drop
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

proxy-bypass

コンテンツの最低限の書き換えを実行し、書き換えるコンテンツのタイプ（外部リンクや XML）を指定するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モードで **proxy-bypass** コマンドを使用します。プロキシのバイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

proxy-bypass interface *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

構文の説明

host	トラフィックの転送先ホストを示します。ホストの IP アドレスまたはホスト名を使用します。
interface	プロキシ バイパス用の ASA インターフェイスを示します。
interface name	ASA インターフェイスを名前で指定します。
link	絶対外部リンクの書き換えを指定します。
none	書き換えを指定しません。
path-mask	一致パターンを指定します。
path-mask	照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ?：任意の 1 文字に一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 128 バイトです。
port	プロキシ バイパス用に予約されているポートを示します。
port number	プロキシ バイパス用に予約されているポート（大きい番号）を指定します。ポートの範囲は 20000 ～ 21000 です。1 つのプロキシ バイパス ルールのみにポートを使用できます。
rewrite	（任意）書き換え用の追加ルール（none、または XML やリンクの組み合わせ）を指定します。
target	トラフィックの転送先リモート サーバを示します。
url	URL を **http(s)://***fully_qualified_domain_name*[:*port*] という形式で入力します。最大 128 バイトです。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。
xml	書き換える XML コンテンツを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ バイパスは、コンテンツの書き換えを最小限に実行して、アプリケーションおよび Web リソースの動作を向上させるために使用します。proxy-bypass コマンドは、セキュリティ アプライアンスを通過する特定の Web アプリケーションの処理方法を決定します。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートがセキュリティ アプライアンスにアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、URL が www.mycompany.com/hrbenefits の場合、*hrbenefits* がパスです。同様に、URL が www.mycompany.com/hrinsurance の場合、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

例

次に、webvpn インターフェイス上のプロキシ バイパス用にポート 20001 を使用するようにセキュリティ アプライアンスを設定する例を示します。HTTP とそのデフォルト ポート 80 を使用してトラフィックを mycompany.site.com に転送し、XML コンテンツを書き換えます。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://mycompany.site.com rewrite xml
```

次に、外部インターフェイスでのプロキシ バイパス用にパス マスク mypath/* を使用するようにセキュリティ アプライアンスを設定する例を示します。HTTP とそのデフォルト ポート 443 を使用してトラフィックを mycompany.site.com に転送し、XML およびリンク コンテンツを書き換えます。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://mycompany.site.com rewrite xml,link
```

関連コマンド

コマンド	説明
apcf	特定アプリケーションに使用する非標準ルールを指定します。
rewrite	トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。

proxy-ldc-issuer

TLS プロキシ ローカル ダイナミック証明書を発行するには、クリプト CA トラストポイント コンフィギュレーション モードで **proxy-ldc-issuer** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

proxy-ldc-issuer

no proxy-ldc-issuer

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

TLS プロキシ ローカル ダイナミック証明書を発行するには、**proxy-ldc-issuer** コマンドを使用します。**proxy-ldc-issuer** コマンドは、クリプト トラストポイントにローカル CA としてのロールを付与して LDC を発行します。クリプト ca トラストポイント コンフィギュレーション モードからアクセスできます。

proxy-ldc-issuer コマンドは、TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。このコマンドは、「enrollment self」のトラストポイントにおいてのみ設定できます。

例

次に、内部ローカル CA を作成し、電話用の LDC を署名する例を示します。このローカル CA は、**proxy-ldc-issuer** がイネーブルな標準の自己署名トラストポイントとして作成されます。

```
hostname(config)# crypto ca trustpoint ldc_server
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# proxy-ldc-issuer
hostname(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
hostname(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
hostname(config-ca-trustpoint)# keypair ldc_signer_key
hostname(config)# crypto ca enroll ldc_server
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

proxy-server

電話プロキシ機能に対して HTTP プロキシを設定するには、電話プロキシ コンフィギュレーション モードで **proxy-server** コマンドを使用します。このコンフィギュレーションは、IP フォンのコンフィギュレーション ファイルの <proxyServerURL> タグの下に書き込まれます。電話プロキシから HTTP プロキシ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

構文の説明

interface *ifc*	セキュリティ アプライアンスで HTTP プロキシが常駐するインターフェイスを指定します。
ip_address	HTTP プロキシの IP アドレスを指定します。
listen_port	HTTP プロキシのリスニング ポートを指定します。指定しない場合、デフォルトは 8080 になります。

デフォルト

リッスン ポートを指定しない場合、ポートはデフォルトで 8080 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

電話プロキシのプロキシ サーバ コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

入力する *ip_address* は、IP フォンおよび HTTP プロキシ サーバの配置場所に基づくグローバル IP アドレスにする必要があります。

プロキシ サーバが DMZ 内にあり、IP 電話がネットワークの外部にある場合、セキュリティ アプライアンスは、NAT ルールが存在するかどうかのルックアップを実行し、グローバル IP アドレスを使用してコンフィギュレーション ファイルに書き込みます。

セキュリティ アプライアンスがホスト名を IP アドレスに解決できる場合は（DNS ルックアップが設定されている場合など）、セキュリティ アプライアンスがそのホスト名を IP アドレスに解決するため、*ip_address* 引数にホスト名を入力できます。

デフォルトでは、エンタープライズ パラメータの下に設定された電話の URL パラメータは、URL 内で FQDN を使用しています。HTTP プロキシ用の DNS lookup で FQDN が解決されない場合は、IP アドレスを使用するようにこれらのパラメータを変更する必要があります。

プロキシ サーバ URL が IP フォンのコンフィギュレーション ファイルに正しく書き込まれたかどうかを確認するには、[Settings] > [Device Configuration] > [HTTP configuration] > [Proxy Server URL] で IP フォンの URL をチェックします。

電話プロキシでは、プロキシ サーバに対するこの HTTP トラフィックを検査しません。

セキュリティ アプライアンスが IP フォンと HTTP プロキシ サーバのパス内にある場合は、既存のデバッグ手法（syslog やキャプチャなど）を使用して、プロキシ サーバをトラブルシューティングします。

電話プロキシが使用中の場合は、プロキシ サーバを 1 つだけ設定できます。ただし、プロキシ サーバを設定した後に IP 電話にコンフィギュレーション ファイルをダウンロードした場合は、IP 電話を再起動して、プロキシ サーバのアドレスが記載されたコンフィギュレーション ファイルが取り込まれるようにする必要があります。

例

次に、**proxy-server** コマンドを使用して電話プロキシ用に HTTP プロキシ サーバを設定する例を示します。

```
hostname(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

publish-crl

ローカル CA が発行した証明書の失効状態を他のセキュリティ アプライアンスが検証できるようにするには、設定 CA サーバ コンフィギュレーション モードで **publish-crl** コマンドを使用します。このコマンドにより、セキュリティ アプライアンスのインターフェイスから CRL を直接ダウンロードできるようになります。CRL をダウンロードできないようにするには、このコマンドの **no** 形式を使用します。

[no] publish-crl interface *interface* **[port** *portnumber* **]**

構文の説明

interface *interface*	インターフェイスに使用される *nameif* を指定します（**gigabitethernet0/1** など）。詳細については、**interface** コマンドを参照してください。
port *portnumber*	任意。インターフェイス デバイスで CRL をダウンロードするときに使用するポートを指定します。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。

デフォルト

デフォルトの **publish-crl** ステータスは、**no publish** です。TCP ポート 80 は、HTTP のデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
設定 CA サーバ	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CRL は、デフォルトでアクセス不可です。必要なインターフェイスおよびポートで CRL ファイルへのアクセスをイネーブルにする必要があります。

TCP ポート 80 は、HTTP のデフォルト ポート番号です。デフォルト以外のポート（ポート 80 以外）を設定する場合は、他のデバイスが新しいポートへのアクセス方法を認識できるように、**cdp-url** コンフィギュレーションにそのポート番号が含まれるようにします。

CRL Distribution Point（CDP; CRL 配布ポイント）は、ローカル CA セキュリティ アプライアンスにおける CRL の場所です。cdp-url コマンドで設定する URL は、発行されるすべての証明書に埋め込まれます。CDP 用に特定の場所を設定しない場合、デフォルトの CDP の URL は http://hostname.domain/+CSCOCA+/asa_ca.crl です。

クライアントレス SSL VPN が同じインターフェイスでイネーブルになっている場合、HTTP リダイレクトと CRL ダウンロード要求は、同じ HTTP リスナーによって処理されます。リスナーは着信 URL をチェックし、cdp-url コマンドで設定した URL と一致する場合に、CRL ファイルがダウンロードされます。URL が cdp-url と一致しない場合は、接続が HTTPS にリダイレクトされます（「http redirect」がイネーブルの場合）。

例

次に、設定 CA サーバ モードで、外部インターフェイスのポート 70 を CRL ダウンロード用にイネーブルにする publish-crl コマンドの例を示します。

次に、設定 CA サーバ モードで、外部のポート 70 を CRL ダウンロード用にイネーブルにする **publish-crl** コマンドの例を示します。

```
hostname(config)# crypto ca server
hostname (config-ca-server)#publish-crl outside 70
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	自動生成される CRL 用に特定の場所を指定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

pwd

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ルート ディレクトリ（/）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**dir** コマンドと機能が類似しています。

例

次に、現在の作業ディレクトリを表示する例を示します。

```
hostname# pwd
disk0:/
hostname# pwd
flash:
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
more	ファイルの内容を表示します。

CHAPTER 23

queue-limit コマンド～ rtp-conformance コマンド

queue-limit（プライオリティ キュー）

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

構文の説明

number-of-packets	キューイング（バッファリング）可能な低遅延または通常のプライオリティのパケットの最大数を指定します。この最大数を超えると、インターフェイスでパケットのドロップが開始されます。指定可能な値の範囲については、「使用上のガイドライン」の項を参照してください。

デフォルト

デフォルトのキューの制限は 1024 パケットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プライオリティ キュー	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、遅延の影響を受けやすい、プライオリティの高いトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）と、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）の 2 つのトラフィック クラスを使用できます。セキュリティ アプライアンスは、プライオリティ トラフィックを認識して、適切な Quality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にする前に、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューを作成する必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドで、プライオリティ キュー モードを開始します。これはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびパケットをドロップする前にバッファに入れることができる両タイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

（注）　インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する*必要があります*。

指定する tx-ring-limit および queue-limit は、プライオリティの高い低遅延キューとベストエフォートキューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの 2 つのパラメータを調整することで、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが、*テールドロップ*です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注）　**queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時にダイナミックに決定されます。この制限を表示するには、コマンド ラインに **help** または **?** と入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論的な最大パケット数は、2147483647 です。

ASA モデル 5505（のみ）では、1 つのインターフェイスにプライオリティ キューを設定すると、他のすべてのインターフェイスで同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけが、すべてのインターフェイスに存在することになります。さらに、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスからも削除されます。

この問題を回避するには、**priority-queue** コマンドを 1 つのインターフェイスにのみ設定します。**queue-limit** コマンドと **tx-ring-limit** コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。

コマンド	説明
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティ キュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。

queue-limit（tcp マップ）

TCP 接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を設定するには、tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

queue-limit *pkt_num* [**timeout** *seconds*]

no queue-limit

構文の説明

pkt_num	TCP 接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を 1 ～ 250 の範囲で指定します。デフォルトは 0 です。この値は、この設定がディセーブルであり、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されることを意味しています。詳細については、「使用上のガイドライン」の項を参照してください。
timeout *seconds*	（任意）順序が不正なパケットをバッファ内に保持可能な最大時間を 1 ～ 20 秒の範囲で設定します。デフォルトは 4 秒です。パケットの順序が不正であり、このタイムアウト期間内に渡されなかった場合、それらのパケットはドロップされます。*pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、制限を 1 以上に設定する必要があります。

デフォルト

デフォルト設定は 0 です。この値は、このコマンドがディセーブルであることを意味しています。

デフォルトのタイムアウトは 4 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)/8.0(4)	**timeout** キーワードが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。

   a. **queue-limit**：tcp マップ コンフィギュレーション モードでは、**queue-limit** コマンドおよびその他数多くのコマンドを入力できます。

2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

TCP 正規化をイネーブルにしない場合、または **queue-limit** コマンドがデフォルトの 0 に設定されている場合（つまりコマンドがディセーブルの場合）、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されます。

- アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP インスペクション再送信（TCP マップ **check-retransmission** コマンド）のための接続のキュー制限は、3 パケットです。セキュリティ アプライアンスが異なるウィンドウ サイズの TCP パケットを受信した場合、キュー制限は、アドバタイズされた設定に合うようにダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

queue-limit コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、TCP パケットからアドバタイズされたすべての設定が**キュー制限**設定を優先して、無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

例

次に、すべての Telnet 接続のキュー制限を 8 パケットに、バッファ タイムアウトを 6 秒に設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8 timeout 6
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

quit

現在のコンフィギュレーション モードを終了したり、特権 EXEC モードやユーザ EXEC モードからログアウトするには、**quit** コマンドを使用します。

quit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **quit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする例を示します。

```
hostname(config)# quit
hostname# quit

Logoff
```

次に、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
hostname(config)# quit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
exit	コンフィギュレーション モードを終了するか、または特権 EXEC モードやユーザ EXEC モードからログアウトします。

radius-common-pw

このセキュリティ アプライアンス経由で特定の RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通パスワードを指定するには、AAA サーバ ホスト モードで **radius-common-pw** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

radius-common-pw *string*

no radius-common-pw

構文の説明

string	この RADIUS サーバにおけるすべての認可トランザクションで共通パスワードとして使用される最大 127 文字の英数字キーワード。大文字と小文字は区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで追加されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバに対してのみ有効です。

RADIUS 認可サーバでは、各接続ユーザに対してパスワードおよびユーザ名が必要です。セキュリティ アプライアンスでは、ユーザ名が自動的に指定されます。ここでは、パスワードを入力します。RADIUS サーバ管理者は、このセキュリティ アプライアンス経由で RADIUS サーバに対して認可を行う各ユーザにこのパスワードが関連付けられるように RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に伝えてください。

共通ユーザ パスワードを指定しない場合、各ユーザのパスワードは各自のユーザ名となります。たとえば、ユーザ名が「jsmith」のユーザは、「jsmith」と入力します。共通ユーザ パスワードにユーザ名を使用する場合は、セキュリティ上の予防措置として、ネットワーク上の他のいずれの場所でもこの RADIUS サーバを認可に使用しないでください。

（注） このフィールドは、実質的には意味がありません。RADIUS サーバはこのフィールドを要求しますが、実際には使用されません。ユーザはこのことを知っている必要はありません。

例

次に、ホスト「1.2.3.4」に「svrgrp1」という名前の RADIUS AAA サーバ グループを設定し、タイムアウト時間を 9 秒に、再試行間隔を 7 秒に、RADIUS 共通パスワードを「allauthpw」に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

radius-reject-message

認証が拒否された場合のログイン画面での RADIUS 拒否メッセージの表示をイネーブルにするには、トンネル グループ webvpn 属性コンフィギュレーション モードで **radius-eject-message** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

radius-reject-message

no radius-reject-message

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

リモート ユーザに対して、認証の失敗についての RADIUS メッセージを表示する場合は、このコマンドをイネーブルにします。

例

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry（削除）

認証中に MS-CHAPv2 を使用してユーザとパスワード アップデートをネゴシエートするようにセキュリティ アプライアンスを設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **radius-with-expiry** コマンドを使用します。RADIUS 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドは無視されます。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

radius-with-expiry

no radius-with-expiry

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換えられました。**radius-with-expiry** コマンドの **no** 形式はサポートされなくなりました。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。

例

次に、設定 ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループに対して radius-with-expiry を設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# radius-with-expiry
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
password-management	パスワード管理をイネーブルにします。**radius-with-expiry** コマンドは、トンネル グループ一般属性コンフィギュレーション モードのこのコマンドに置き換えられました。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

ras-rcf-pinholes

ゲートキーパーがネットワーク内にある場合に、H.323 エンドポイント間でのコール設定をイネーブルにするには、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ras-rcf-pinholes enable

no ras-rcf-pinholes enable

構文の説明

enable	H.323 エンドポイント間でのコール設定をイネーブルにします。

デフォルト

デフォルトでは、このオプションは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスには、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、セキュリティ アプライアンスは発信元 IP アドレス / ポート 0/0 を通じてピンホールを開きます。

例

次に、ポリシー マップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ras-rcf-pinholes enable
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

rate-limit

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **rate-limit** コマンドを使用して、**match** コマンドまたはクラス マップに一致するパケットのメッセージのレートを制限します。このレート制限アクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでこのアクションが可能なわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

構文の説明

messages_per_second	1 秒あたりのメッセージ数を制限します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**rate-limit** コマンドを入力して、メッセージのレートを制限できます。

レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。ここで dns_policy_map はインスペクション ポリシー マップの名前です。

例

次に、invite 要求を 1 秒あたり 100 メッセージに制限する例を示します。

```
hostname(config-cmap)# policy-map type inspect sip sip-map1
hostname(config-pmap-c)# match request-method invite
hostname(config-pmap-c)# rate-limit 100
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

reactivation-mode

グループ内の障害が発生したサーバを再アクティブ化する方法を指定するには、AAA サーバ プロトコル モードで **reactivation-mode** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

構文の説明

deadtime *minutes*	（任意）グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバが非アクティブになった後でのみ、障害が発生したサーバを再アクティブ化します。
timed	30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

デフォルト

デフォルトの再アクティブ化モードは depletion で、デフォルトの deadtime の値は 10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ プロトコル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各サーバ グループには、所属するサーバの再アクティブ化ポリシーを指定する属性があります。

depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。**depletion** モードが使用されている場合は、**deadtime** パラメータも指定できます。**deadtime** パラメータは、グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を分単位で指定します。このパラメータは、サーバ グループがローカル フォールバック機能とともに使用されている場合にのみ意味があります。

timed モードでは、障害が発生したサーバは、30 秒のダウン時間の後に再アクティブ化されます。このモードは、サーバ リスト内の最初のサーバをプライマリ サーバとして使用しており、このサーバを可能な限りオンラインに維持する必要がある場合に役立ちます。このポリシーは、UDP サーバの場合

は機能しません。UDP サーバへの接続は、たとえそのサーバが存在しない場合でも失敗しないため、UDP サーバは無条件にオンラインに戻ります。サーバ リストに到達不能な複数のサーバが含まれている場合には、接続時間が遅延したり、接続に失敗する場合があります。

同時アカウンティングがイネーブルになっているアカウンティング サーバ グループでは、**timed** モードが強制的に使用されます。このことは、特定のリスト内のすべてのサーバが同等に扱われることを意味しています。

例

次に、「srvgrp1」という名前の TACACS+ AAA サーバで、再アクティブ化モードを depletion に、deadtime を 15 分に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

次に、「srvgrp1」という名前の TACACS+ AAA サーバで timed 再アクティブ化モードを使用するように設定する例を示します。

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)#
```

関連コマンド

accounting-mode	アカウンティング メッセージが単一のサーバに送信されるか、またはグループ内のすべてのサーバに送信されるかを示します。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始して、グループ内のすべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できるようにします。
max-failed-attempts	サーバ グループ内の所定のサーバが非アクティブ化されるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

record-entry

CTL ファイルの作成に使用されるトラストポイントを指定するには、CTL ファイル コンフィギュレーション モードで record-entry コマンドを使用します。CTL からレコード エントリを削除するには、このコマンドの **no** 形式を使用します。

record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

no record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trust_point* **address** *ip_address* [**domain-name** *domain_name*]

構文の説明

capf	このトラストポイントのロールを CAPF に指定します。1 つの CAPF トラストポイントのみを設定できます。
cucm	このトラストポイントのロールを CCM に指定します。複数の CCM トラストポイントを設定できます。
cucm-tftp	このトラストポイントのロールを CCM+TFTP に指定します。複数の CCM+TFTP トラストポイントを設定できます。
domain-name *domain_name*	（任意）トラストポイントの DNS フィールドの作成に使用されるトラストポイントのドメイン名を指定します。この名前は、サブジェクト DN の一般名フィールドに追加されて、DNS 名が作成されます。トラストポイントに FQDN が設定されていない場合は、ドメイン名を設定する必要があります。
address *ip_address*	トラストポイントの IP アドレスを指定します。
tftp	このトラストポイントのロールを TFTP に指定します。複数の TFTP トラストポイントを設定できます。
trustpoint *trust_point*	インストールされているトラストポイントの名前を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL ファイル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

domain-name は、1 つのみ指定できます。CTL ファイルが存在しない場合は、手動でこの証明書を CUCM からセキュリティ アプライアンスにエクスポートします。

このコマンドは、電話プロキシの CTL ファイルを設定していない場合にのみ使用します。すでに CTL ファイルを設定している場合は、このコマンドを使用しないでください。

ip_address 引数に指定する IP アドレスは、トラストポイントの CTL レコードで使用される IP アドレスとなるため、グローバル アドレス、または IP Phone によって認識されるアドレスである必要があります。

CTL ファイルで必要な各エントリに対して、さらに record-entry コンフィギュレーションを追加します。

例

次に、**record-entry** コマンドを使用して、CTL ファイルの作成に使用されるトラストポイントを指定する例を示します。

```
hostname(config-ctl-file)# record-entry cucm-tftp trustpoint cucm1 address 192.168.1.2
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

redirect-fqdn

VPN ロード バランシング モードで完全修飾ドメイン名を使用したリダイレクトをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。

redirect-fqdn {enable | disable}

no redirect-fqdn {enable | disable}

（注）　VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

disable	完全修飾ドメイン名を使用したリダイレクトをディセーブルにします。
enable	完全修飾ドメイン名を使用したリダイレクトをイネーブルにします。

デフォルト

この動作は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロード バランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。

VPN クラスタ マスターとして、セキュリティ アプライアンスは、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別のセキュリティ アプライアンス）の外部 IP アドレスではなく Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく FQDN を使用して WebVPN ロード バランシングを実行するには、次の設定手順を実行する必要があります。

ステップ 1　**redirect-fqdn enable** コマンドを使用して、ロード バランシングにおける FQDN の使用をイネーブルにします。

ステップ 2　DNS サーバに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　dns domain-lookup inside コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバへのルートを持つ任意のインターフェイスを指定します。

ステップ 4　`dns name-server 10.2.3.4` のように、ASA に DNS サーバの IP アドレスを定義します（10.2.3.4 は、DNS サーバの IP アドレス）。

例

次に、リダイレクトをディセーブルにする **redirect-fqdn** コマンドの例を示します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn disable
hostname(config-load-balancing)#
```

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを「test」と指定し、クラスタのプライベート インターフェイスを「foo」と指定するインターフェイス コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。

コマンド	説明
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

redistribute（EIGRP）

1 つのルーティング ドメインから EIGRP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

構文の説明

bandwidth	EIGRP 帯域幅メトリック（キロビット/秒）。有効な値は、1 ～ 4294967295 です。
connected	インターフェイスに接続されているネットワークを EIGRP ルーティング プロセスに再配布することを指定します。
delay	EIGRP 遅延メトリック（10 マイクロ秒単位）有効な値は、0 ～ 4294967295 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
load	EIGRP 有効帯域幅（負荷）メトリック。有効な値は、1 ～ 255 です（255 は 100% の負荷を示します）。
match	（任意）OSPF から EIGRP にルートを再配布する条件を指定します。
metric	（任意）EIGRP ルーティング プロセスに再配布されるルートの EIGRP メトリックの値を指定します。
mtu	パスの MTU。有効な値は 1 ～ 65535 です。
nssa-external *type*	NSSA の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	EIGRP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
reliability	EIGRP 信頼性メトリック。有効な値は、0 ～ 255 です（255 は 100% の信頼性を示します）。
rip	RIP ルーティング プロセスから EIGRP ルーティング プロセスへのネットワークの再配布を指定します。
route-map *map_name*	（任意）送信元ルーティング プロトコルから EIGRP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルートマップの名前。指定しない場合は、すべてのルートが再配布されます。
static	EIGRP ルーティング プロセスにスタティック ルートを再配布するために使用します。

デフォルト

コマンドのデフォルトは次のとおりです。

- **match**：**Internal**、**external 1**、**external 2**

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン　EIGRP コンフィギュレーションに **default-metric** コマンドを設定していない場合は、redistribute コマンドで **metric** を指定する必要があります。

例　次に、スタティック ルートおよび接続ルートを EIGRP ルーティング プロセスに再配布する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# redistribute static
hostname(config-router)# redistribute connected
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（OSPF）

1 つのルーティング ドメインから OSPF ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected** | **eigrp** *as-number*} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

構文の説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	OSPF ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効な値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を指定します。
metric *metric_value*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type *metric_type*	（任意）OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられている外部リンク タイプ。**1**（タイプ 1 外部ルート）または **2**（タイプ 2 外部ルート）を指定できます。
nssa-external *type*	NSSA の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	現在の OSPF ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
rip	RIP ルーティング プロセスから現在の OSPF ルーティング プロセスへのネットワークの再配布を指定します。
route-map *map_name*	（任意）送信元ルーティング プロトコルから現在の OSPF ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルート マップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。

subnets	（任意）OSPF へのルートの再配布において、指定したプロトコルの再配布の範囲を指定します。使用しない場合は、クラスフル ルートのみが再配布されます。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **metric-type** *type-value*：**2**
- **match**：**Internal**、**external 1**、**external 2**
- **tag** *tag-value*：0

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは、**rip** キーワードを含むように変更されました。
8.0(2)	このコマンドが、**eigrp** キーワードを含めるように修正されました。

例

次に、スタティック ルートを現在の OSPF プロセスに再配布する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute static
```

関連コマンド

コマンド	説明
redistribute（RIP）	RIP ルーティング プロセスにルートを再配布します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（RIP）

別のルーティング ドメインから RIP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

構文の説明

connected	インターフェイスに接続されているネットワークを RIP ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	RIP ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効な値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）OSPF から RIP にルートを再配布する条件を指定します。
metric {*metric_value* | **transparent**}	（任意）再配布するルートの RIP メトリック値を指定します。*metric_value* の有効な値は、0 ～ 16 です。メトリックを **transparent** に設定すると、現在のルート メトリックが使用されます。
nssa-external *type*	Not-So-Stubby Area（NSSA）の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	RIP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
route-map *map_name*	（任意）送信元ルーティング プロトコルから RIP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルート マップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを RIP プロセスに再配布するために使用されます。

デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **match**：**Internal**、**external 1**、**external 2**

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	このコマンドが、**eigrp** キーワードを含めるように修正されました。

例　次に、スタティック ルートを現在の RIP プロセスに再配布する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# redistribute static metric 2
```

関連コマンド

コマンド	説明
redistribute（EIGRP）	他のルーティング ドメインから EIGRP にルートを再配布します。
redistribute（OSPF）	他のルーティング ドメインから OSPF にルートを再配布します。
router rip	RIP ルーティング プロセスをイネーブルにして、そのプロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redundant-interface

冗長インターフェイスのうちのどのメンバー インターフェイスをアクティブにするかを設定するには、特権 EXEC モードで **redundant-interface** コマンドを使用します。

redundant-interface redundant*number* **active-member** *physical_interface*

構文の説明

active-member *physical_interface*	アクティブ メンバーを設定します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。
redundant*number*	冗長インターフェイス ID（**redundant1** など）を指定します。

デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバー インターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

```
hostname# show interface redundantnumber detail | grep Member
```

次に例を示します。

```
hostname# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

例

次に、冗長インターフェイスを作成する例を示します。デフォルトでは、gigabitethernet 0/0 がコンフィギュレーション内の最初のインターフェイスであるため、このインターフェイスがアクティブです。redundant-interface コマンドでは、gigabitethernet 0/1 をアクティブ インターフェイスに設定しています。

```
hostname(config-if)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1

hostname(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
member-interface	冗長インターフェイス ペアにメンバー インターフェイスを割り当てます。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

regex

テキストを照合する正規表現を作成するには、グローバル コンフィギュレーション モードで **regex** コマンドを使用します。正規表現を削除するには、このコマンドの **no** 形式を使用します。

regex *name regular_expression*

no regex *name* [*regular_expression*]

構文の説明

name	正規表現名を最大 40 文字で指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

regex コマンドは、テキスト照合が必要なさまざまな機能で使用できます。たとえば、*インスペクション ポリシー マップ*を使用して、モジュラ ポリシー フレームワーク を使用したアプリケーション インスペクションの特別なアクションを設定できます（**policy map type inspect** コマンドを参照）。インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラス マップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現は、正規表現クラス マップにグループ化できます（**class-map type regex** コマンドを参照）。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して、特定のアプリケーション トラフィックの内容（HTTP パケット内の本文テキストなど）を照合できます。

（注）　最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

表 23-1 に、特別な意味を持つメタ文字の一覧を示します。

表 23-1　　regex メタ文字

文字	説明	注意事項
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp***)**	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）**　Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc***]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。

表 23-1　regex メタ文字 （続き）

文字	説明	注意事項
[*a-c***]**	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**" test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	Tab	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

正規表現が想定どおりに一致するかどうかをテストするには、**test regex** コマンドを入力します。

正規表現のパフォーマンスへの影響は、主に次の 2 つの要因によって決定されます。

- 正規表現照合で検索される必要があるテキストの長さ。

  検索長が短い場合は、正規表現エンジンのセキュリティ アプライアンスに対するパフォーマンス上の影響は小さくなります。

- 正規表現照合で検索される必要がある正規表現チェーン テーブルの数。

検索長のパフォーマンスへの影響

正規表現検索を設定すると、通常は、検索対象テキストのすべてのバイトが正規表現データベースに対して検査されて、一致が検索されます。検索対象テキストが長くなるほど、検索時間も長くなります。次に、この現象を表すパフォーマンス テスト ケースを示します。

- ある HTTP トランザクションでは、1 回の 300 バイトの GET 要求と 1 回の 3250 バイトの応答が行われます。
- URI 検索には 445 の正規表現が、要求本文検索には 34 の正規表現が使用されます。
- 応答本文検索には 55 の正規表現が使用されます。

URI および HTTP GET 要求の本文のみを検索するようにポリシーを設定すると、スループットは次のようになります。

- 対応する正規表現データベースが検索されない場合は 420 mbps。
- 対応する正規表現データベースが検索される場合は 413 mbps（正規表現を使用するオーバーヘッドが比較的小さいことがわかります）。

ただし、HTTP 応答本文全体も検索するようにポリシーを設定すると、応答本文の検索対象が長いため（3250 バイト）、スループットは 145 mbps まで低下します。

正規表現検索のテキスト長が長くなる要因は次のとおりです。

- 複数の異なるプロトコル フィールドに対して正規表現検索が設定されている場合。たとえば、HTTP インスペクションでは、URI にのみ正規表現照合が設定されていると、URI フィールドのみが正規表現照合のために検索され、検索長は URI 長に制限されます。ただし、ヘッダーや本文などの他のプロトコル フィールドにも正規表現照合が設定されていると、ヘッダー長や本文長の分だけ検索長が長くなります。
- 検索対象のフィールドが長い場合。たとえば、URI に正規表現検索が設定されている場合、GET 要求内の長い URI の検索長は長くなります。また、現在、HTTP 本文の検索長はデフォルトで 200 バイトまでに制限されています。ただし、本文を検索するようにポリシーを設定し、本文検索長が 5000 バイトに変更されると、本文検索が長くなるため、パフォーマンスに対して大きな影響があります。

正規表現チェーン テーブル数のパフォーマンスへの影響

現在、同じプロトコル フィールドに設定されたすべての正規表現（URI に対するすべての正規表現など）は、1 つ以上の正規表現チェーン テーブルで構成されるデータベースに構築されます。テーブルの数は、必要な合計メモリ量、およびテーブル構築時に使用可能なメモリ量によって決定されます。次のいずれかの条件が満たされる場合、正規表現データベースは複数のテーブルに分割されます。

- 必要な合計メモリが 32 MB を超える場合。これは、最大テーブル サイズが 32 MB に制限されているためです。
- 最大連続メモリ サイズが正規表現データベース全体を構築するのに十分ではない場合、複数の小さなテーブルが構築されて、それらのテーブルにすべての正規表現が格納されます。メモリ フラグメンテーションの程度は、相互に関連する数多くの要因によって左右されるため、フラグメンテーションのレベルを予測することは事実上不可能です。

複数のチェーン テーブルがある場合、正規表現照合において各テーブルが検索される必要があるため、検索時間は検索対象のテーブル数に比例して長くなります。

特定のタイプの正規表現では、テーブル サイズが大幅に増加する傾向があります。可能な限りワイルドカードおよび繰り返し要素を避けるように正規表現を設計することを推奨します。次のメタ文字については、表 23-1 を参照してください。

- ワイルドカード タイプの指定を伴う正規表現
  - ドット（.）
- クラス内の任意の文字に一致するさまざまな文字クラス
  - [^a-z]
  - [a-z]
  - [abc]]
- 繰り返しタイプの指定を伴う正規表現
  - *
  - +
  - {n,}

- 次のようにワイルドカード タイプの正規表現と繰り返しタイプの正規表現を組み合わせると、テーブル サイズが大幅に増加する可能性があります。
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.*（これは、「123」と照合することと同じであるため、このような指定は行わないでください）。

次に、ワイルドカードや繰り返しの有無によって正規表現のメモリ使用量がどのように異なるかについての例を示します。

- 次の 4 つの正規表現のデータベース サイズは 958,464 バイトです。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 次の 4 つの正規表現のデータベース サイズはわずか 10240 バイトです。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

正規表現の数が増えると、正規表現データベースで必要になる合計メモリ量も増え、そのためメモリがフラグメント化されている場合にはより多くのテーブル数が必要になる可能性があります。次に、異なる正規表現数でのメモリ使用量の例を示します。

- 100 サンプル URI : 3,079,168 バイト
- 200 サンプル URI : 7,156,224 バイト
- 500 サンプル URI : 11,198,971 バイト

（注） コンテキストごとの最大正規表現数は 2048 です。

debug menu regex 40 10 コマンドを使用して、各正規表現データベースにおけるチェーン テーブル数を表示できます。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックと照合するインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。

コマンド	説明
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
test regex	正規表現をテストします。

reload

リブートしてコンフィギュレーションをリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm***]** [**max-hold-time** [*hh*:]*mm***]** [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

構文の説明

at *hh*:*mm*	（任意）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定しない場合、リロードは、指定時刻が現在時刻よりも後の場合は当日の指定時刻に、指定時刻が現在時刻よりも前の場合は翌日の指定時刻に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 時間以内に実行される必要があります。
cancel	（任意）スケジューリングされているリロードをキャンセルします。
day	（任意）1 ～ 31 の範囲で日付を指定します。
in [*hh*:]*mm*]	（任意）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、24 時間以内に実行される必要があります。
max-hold-time [*hh*:]*mm*	（任意）シャットダウンまたはリブートの前に他のサブシステムに対して通知するためにセキュリティ アプライアンスが待機する最大ホールド タイムを指定します。この時間が経過すると、（強制）クイック シャットダウンまたはリブートが実行されます。
month	（任意）月の名前を指定します。月の名前を表す一意のストリングを作成するために十分な文字を入力します。たとえば、「Ju」は、June または July を表すことができるため一意ではありませんが、「Jul」は一意です。これは、「Jul」で始まる月は「July」しかないためです。
noconfirm	（任意）ユーザの確認なしでリロードすることをセキュリティ アプライアンスに許可します。
quick	（任意）すべてのサブシステムに対して通知や適切なシャットダウンを行わないで、強制的にクイック リロードを行います。
reason *text*	（任意）リロードの理由を 1 ～ 255 文字で指定します。理由のテキストは、すべての開いている IPSec VPN クライアント、端末、コンソール、telnet、SSH、および ASDM 接続またはセッションに送信されます。 **（注）** isakmp などの一部のアプリケーションでは、IPSec VPN クライアントに理由のテキストを送信するために追加のコンフィギュレーションが必要となります。詳細については、ソフトウェア コンフィギュレーション マニュアルの該当する項を参照してください。
save-config	（任意）シャットダウンの前に、実行コンフィギュレーションをメモリに保存します。**save-config** キーワードを入力しない場合、未保存のコンフィギュレーションの変更はリロード後にすべて失われます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されて、*day*、*hh*、*mm*、*month*、**quick**、**save-config**、および *text* という新しい引数およびキーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンス がリブートし、フラッシュからコンフィギュレーションがリロードされます。

デフォルトで、**reload** コマンドは対話形式です。セキュリティ アプライアンスは、まずコンフィギュレーションが変更されており、未保存であるかどうかをチェックします。変更が未保存の場合、コンフィギュレーションを保存するように求めるプロンプトがセキュリティ アプライアンスによって表示されます。マルチ コンテキスト モードでは、セキュリティ アプライアンスによって、未保存のコンフィギュレーションがある各コンテキストに対してプロンプトが表示されます。**save-config** パラメータを指定すると、コンフィギュレーションはプロンプトなしで保存されます。次に、システムのリロードを確認するプロンプトがセキュリティ アプライアンスによって表示されます。**y** と入力するか、または Enter キーを押した場合にのみリロードが行われます。確認後、セキュリティ アプライアンスは、遅延パラメータ（**in** または **at**）を指定したかどうかに応じて、リロード プロセスを開始またはスケジューリングします。

デフォルトで、リロード プロセスは「グレースフル」（「ナイス」とも呼ばれます）モードで動作します。すべての登録されているサブシステムは、リブート実行の前に通知されるため、リブート前に適切にシャットダウンできます。このようなシャットダウンが行われるのを待機しない場合は、**max-hold-time** パラメータを指定して、待機する最大時間を指定します。または、**quick** パラメータを使用して、影響のあるサブシステムへの通知やグレースフル シャットダウンの待機を行わずに、すぐに強制的にリロード プロセスを開始できます。

noconfirm パラメータを指定すると、**reload** コマンドを非対話形式で実行できます。この場合、セキュリティ アプライアンスでは、**save-config** パラメータを指定していない限り、未保存のコンフィギュレーションがあるかどうかはチェックされません。また、セキュリティ アプライアンスでは、システムのリブート前にユーザに対して確認を求めるプロンプトは表示されません。遅延パラメータを指定していない限り、リロード プロセスがすぐに開始またはスケジューリングされます。ただし、**max-hold-time** パラメータまたは **quick** パラメータを指定して、動作またはリロード プロセスを制御できます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** を使用します。すでに進行中のリロードはキャンセルできません。

（注） フラッシュ パーティションに書き込まれていない設定変更は、リロード後に失われます。リブート前に、**write memory** コマンドを入力して、現在の設定をフラッシュ パーティションに保存してください。

例

次の例は、コンフィギュレーションをリブートおよびリロードする方法を示しています。

```
hostname# reload
```

```
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	セキュリティ アプライアンスのリロード ステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモート アクセス セッションの数を指定します。この数を超えると、セキュリティ アプライアンスによってトラップが送信されます。

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

構文の説明

threshold-value	セキュリティ アプライアンスでサポートされるセッションの制限数以下の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0 (1)	このコマンドが導入されました。

例

次に、しきい値を 1500 に設定する例を示します。

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値によるトラッピングをイネーブルにします。

rename

ファイルまたはディレクトリの名前をある名前から別の名前に変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename /noconfirm/ /disk0: | disk1: | flash:/ ***source-path*** **[disk0: | disk1: | flash:/** ***destination-path***

構文の説明

/noconfirm	（任意）確認プロンプトを表示しないようにします。
destination-path	新しいファイル名のパスを指定します。
disk0*:*	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
source-path	元のファイル名のパスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

rename flash: flash: コマンドを入力すると、元のファイル名および新しいファイル名を入力するように求められます。

ファイル システムにまたがってファイルやディレクトリの名前を変更することはできません。

次に例を示します。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次に、「test」というファイル名を「test1」に変更する例を示します。

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイル システムに関する情報を表示します。

rename（クラス マップ）

クラス マップの名前を変更するには、クラス マップ コンフィギュレーション モードで **rename** コマンドを入力します。

rename *new_name*

構文の説明

new_name	クラス マップの新しい名前を最大 40 文字で指定します。「class-default」という名前は予約されています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、test というクラス マップの名前を test2 に変更する例を示します。

```
hostname(config)# class-map test
hostname(config-cmap)# rename test2
```

関連コマンド

コマンド	説明
class-map	クラス マップを作成します。

renewal-reminder

ローカルの Certificate Authority（CA; 認証局）証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定するには、CA サーバ コンフィギュレーション モードで **renewal-reminder** コマンドを使用します。期間をデフォルトの 14 日にリセットするには、このコマンドの **no** 形式を使用します。

renewal-reminder *time*

no renewal-reminder

構文の説明

time	発行されている証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定します。有効な値の範囲は、1 ～ 90 日です。

デフォルト

デフォルトで、CA サーバは、証明書が期限切れになる 14 日前に再登録を求める有効期限通知およびリマインダを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

証明書有効期限 - 更新リマインダ日数の時点、（有効期限 + ワンタイム パスワード有効期限）- 更新リマインダ日数 / 2 の時点、および（有効期限 + ワンタイム パスワード有効期限）- 更新リマインダ日数 / 4 の時点の合計 3 回のリマインダが送信されます。

ユーザ データベースに電子メール アドレスが指定されている場合は、3 回の各リマインダにおいて、電子メールが証明書所有者に自動的に送信されます。電子メール アドレスが存在しない場合は、更新を管理者に通知する syslog メッセージが生成されます。

例

次に、証明書有効期限の 7 日前にセキュリティ アプライアンスからユーザに対して有効期限通知を送信するように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# renewal-reminder 7
hostname(config-ca-server)#
```

次に、有効期限通知のタイミングをデフォルトである証明書有効期限の 14 日前にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no renewal-reminder
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
lifetime	CA 証明書、すべての発行されている証明書、および CRL のライフタイムを指定します。
show crypto ca server	ローカル CA サーバのコンフィギュレーション詳細を表示します。

replication http

フェールオーバー グループに対して HTTP 接続のレプリケーションをイネーブルにするには、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

replication http

no replication http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**replication http** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー コンフィギュレーションのフェールオーバー グループに対するコマンドであることを除いて、Active/Standby フェールオーバー用の **failover replication http** コマンドと同じ機能を備えています。

例

次の例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover replication http	HTTP 接続を複製するためのステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内の特定のコマンドを禁止するには、FTP マップ コンフィギュレーション モードで **request-command deny** コマンドを使用します。FTP マップ コンフィギュレーション モードには、**ftp-map** コマンドを使用してアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

構文の説明

appe	ファイルへの追加を行うコマンドを拒否します。
cdup	現在の作業ディレクトリの親ディレクトリに移動するコマンドを拒否します。
dele	サーバのファイルを削除するコマンドを拒否します。
get	サーバからファイルを取得するクライアント コマンドを拒否します。
help	ヘルプ情報を提供するコマンドを拒否します。
mkd	サーバ上にディレクトリを作成するコマンドを拒否します。
put	サーバにファイルを送信するクライアント コマンドを拒否します。
rmd	サーバ上のディレクトリを削除するコマンドを拒否します。
rnfr	変更元ファイル名を指定するコマンドを拒否します。
rnto	変更先ファイル名を指定するコマンドを拒否します。
site	サーバ システムに固有のコマンドを禁止します。通常、リモート管理に使用します。
stou	固有のファイル名を使用してファイルを保存するコマンドを拒否します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
FTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ストリクト FTP インスペクションを使用する場合に、セキュリティ アプライアンスを通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例

次に、**stor**、**stou**、または **appe** コマンドを含む FTP 要求をセキュリティ アプライアンスでドロップする例を示します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。
mask-syst-reply	FTP サーバ応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

request-data-size

SLA 動作要求パケットのペイロードのサイズを設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **request-data-size** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-data-size *bytes*

no request-data-size

構文の説明

bytes	要求パケットのペイロードのサイズ（バイト単位）。有効な値は、0 ～ 16384 です。最小値は、使用するプロトコルに応じて異なります。エコー タイプでは、最小値は 28 バイトです。プロトコルまたは PMTU で許可されている最大値よりも大きい値を設定しないでください。 **（注）** セキュリティ アプライアンスによって 8 バイトのタイムスタンプがペイロードに追加されるため、実際のペイロードは *bytes* + 8 バイトになります。

デフォルト

デフォルトの *bytes* は 28 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

到達可能性を確保するために、デフォルトのデータ サイズを大きくして、送信元と宛先との間の PMTU の変化を検出する必要がある場合があります。PMTU が低いと、セッションのパフォーマンスに影響を与える可能性が高くなります。また、低い PMTU が検出された場合は、セカンダリ パスが使用されることを示している可能性があります。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
```

```
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

request-queue

応答を待機する GTP 要求のキューイング可能最大数を指定するには、GTP マップ コンフィギュレーション モードで **request-queue** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスします。この数字をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*

no request-queue *max_requests*

構文の説明

max_requests	応答を待機する GTP 要求のキューイング可能最大数。値の範囲は、1 ～ 4294967295 です。

デフォルト

max_requests のデフォルトは 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gtp request-queue コマンドは、応答を待機する GTP 要求のキューイング可能最大数を指定します。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。

例

次に、300 バイトの最大要求キュー サイズを指定する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

request-timeout

失敗した SSO 認証試行がタイムアウトになるまでの秒数を設定するには、webvpn コンフィギュレーション モードで **request-timeout** コマンドを使用します。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-timeout *seconds*

no request-timeout

構文の説明

seconds	失敗した SSO 認証の試行がタイムアウトするまでの秒数。指定できる範囲は 1 ～ 30 秒です。小数の値はサポートされていません。

デフォルト

このコマンドのデフォルト値は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。現在、セキュリティ アプライアンスでは、SiteMinder-type および SAML POST-type の SSO サーバがサポートされています。

このコマンドは SSO サーバの両タイプに適用されます。

SSO 認証をサポートするようにセキュリティ アプライアンスを設定した後、2 つのタイムアウト パラメータを調整できます。

- 失敗した SSO 認証試行がタイムアウトになるまでの秒数（**request-timeout** コマンドを使用）。
- 失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数（**max-retry-attempts** コマンドを参照）。

例

次に、webvpn 設定 sso siteminder モードで、SiteMinder-type SSO サーバ「example」の認証タイムアウトを 10 秒に設定する例を示します。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# request-timeout 10
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

reserve-port-protect

メディア ネゴシエーション中の予約ポートの使用を制限するには、パラメータ コンフィギュレーション モードで **reserve-port-protect** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

reserve-port-protect

no reserve-port-protect

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、RTSP インスペクション ポリシー マップで予約ポートを保護する例を示します。

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# reserve-port-protect
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

reserved-bits

TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりするには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

構文の説明

allow	TCP ヘッダーの予約ビットが設定されているパケットを許可します。
clear	TCP ヘッダーの予約ビットをクリアして、パケットを許可します。
drop	TCP ヘッダーの予約ビットが設定されているパケットをドロップします。

デフォルト

デフォルトで、予約ビットは許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。末端のホストにおける予約ビットが設定されているパケットの処理方法を明確に指定するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。処理方法が明確に指定されていないと、セキュリティ アプライアンスが同期化されていない状態になる可能性があります。TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりできます。

例

次に、すべての TCP フローにおいて、予約ビットが設定されているパケットをクリアする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

reset

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **reset** コマンドを使用して、**match** コマンドまたはクラス マップに一致するトラフィックに対してパケットをドロップし、接続を閉じて、TCP リセットを送信します。このリセット アクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでこのアクションが可能なわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

reset [**log**]

no reset [**log**]

構文の説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**reset** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するトラフィックに対してパケットをドロップし、接続を閉じることができます。

接続をリセットした後は、インスペクション ポリシー マップのアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドまたは **class** コマンドとの照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます 同じ **match** または **class** コマンドに対して **reset** アクションと **log** アクションの両方を設定できます。この場合、パケットは、特定の一致において、ログに記録されてからリセットされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、http-traffic クラス マップに一致した場合に、接続をリセットして、ログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

retries

セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

retries *number*

no retries [*number*]

構文の説明

number	再試行回数を 0 ～ 10 の範囲で指定します。デフォルトは 2 です。

デフォルト

デフォルトの再試行回数は 2 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

name-server コマンドを使用して DNS サーバを追加します。

dns name-server コマンドがこのコマンドに置き換えられました。

例

次に、再試行回数を 0 回に設定する例を示します。セキュリティ アプライアンスは各サーバへの要求を 1 回のみ行います。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns retries 0
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループ モードを開始します。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

retry-interval

指定済みの aaa-server host コマンドで指定されている特定の AAA サーバへの再試行間隔を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。再試行間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

retry-interval *seconds*

no retry-interval

構文の説明

seconds	要求の再試行間隔（1 ～ 10 秒）を指定します。これは、セキュリティ アプライアンスが接続要求を再試行するまでに待機する時間です。

デフォルト

デフォルトの再試行間隔は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

接続試行間にセキュリティ アプライアンスが待機する秒数を指定またはリセットするには、**retry-interval** コマンドを使用します。セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。

例

次に、コンテキストでの **retry-interval** コマンドの例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。

show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。
timeout	セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定します。

reval-period

NAC フレームワーク セッションにおける成功した各ポスチャ検証間の間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **reval-period** コマンドを使用します。このコマンドを NAC フレームワーク ポリシーから削除するには、このコマンドの **no** 形式を使用します。

reval-period *seconds*

no reval-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 300 ～ 86400 です。

デフォルト

デフォルト値は 36000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ポスチャ検証に成功するたびに、再検証タイマーが開始されます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスでは、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。

例

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
hostname(config-nac-policy-nac-framework)# reval-period 86400
hostname(config-nac-policy-nac-framework)
```

次に、NAC ポリシーから再検証タイマーを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no reval-period
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。

revert webvpn all

セキュリティ アプライアンス のフラッシュ メモリから、すべての Web 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除するには、特権 EXEC モードで **revert webvpn all** コマンドを入力します。

revert webvpn all

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスのフラッシュ メモリから Web 関連のすべての情報（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）をディセーブルにし、削除するには、**revert webvpn all** コマンドを使用します。すべての Web 関連データを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、セキュリティ アプライアンスからすべての Web 関連コンフィギュレーション データを削除するコマンドを示します。

```
hostname# revert webvpn all
hostname
```

関連コマンド

コマンド	説明
show import webvpn (*任意*)	このコマンドは、セキュリティ アプライアンス上のフラッシュ メモリにそのとき存在する、さまざまなインポートされた WebVPN データおよびプラグインを表示します。

revert webvpn customization

セキュリティ アプライアンスのキャッシュ メモリからカスタマイゼーション オブジェクトを削除するには、特権 EXEC モードで **revert webvpn customization** コマンドを入力します。

revert webvpn customization *name*

構文の説明

name	削除するカスタマイゼーション オブジェクトの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

指定したカスタマイゼーションのリモート クライアントレス SSL VPN サポートを削除し、セキュリティ アプライアンスのキャッシュ メモリからそのカスタマイゼーション オブジェクトを削除するには、**revert webvpn customization** コマンドを使用します。カスタマイゼーション オブジェクトを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。カスタマイゼーション オブジェクトには、特定の指定されたポータル ページのコンフィギュレーション パラメータが含まれています。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションの設定機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。セキュリティ アプライアンスでは、8.0 ソフトウェアへのアップグレード時に、古い設定を使用して新しいカスタマイゼーション オブジェクトを生成することによって、現在の設定が保持されます。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

（注） バージョン 7.2 のポータル カスタマイゼーションおよび URL リストは、バージョン 8.0 へのアップグレード前にバージョン 7.2(x) のコンフィギュレーション ファイルで適切なインターフェイスにおいてクライアントレス SSL VPN（WebVPN）がイネーブルになっている場合にのみ、ベータ 8.0 コンフィギュレーションで動作します。

例

次に、GroupB という名前のカスタマイゼーション オブジェクトを削除するコマンドを示します。

```
hostname# revert webvpn customization groupb
```

hostname

関連コマンド

コマンド	説明
customization	トンネル グループ、グループ、またはユーザに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	セキュリティ アプライアンスのフラッシュ デバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn plug-in protocol

セキュリティ アプライアンスのフラッシュ デバイスからプラグインを削除するには、特権 EXEC モードで **revert webvpn plug-in protocol** コマンドを入力します。

revert plug-in protocol *protocol*

構文の説明

protocol	次のいずれかのストリングを入力します。 • **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。 • **ssh** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

指定した Java ベースのクライアント アプリケーションのクライアントレス SSL VPN サポートをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ ドライブからも削除するには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次に、RDP のサポートを削除するコマンドを示します。

```
hostname# revert webvpn plug-in protocol rdp
hostname
```

関連コマンド

コマンド	説明
`import webvpn plug-in protocol`	指定したプラグインを URL からセキュリティ アプライアンスのフラッシュ デバイスにコピーします。このコマンドを発行すると、クライアントレス SSL VPN での今後のセッションにおいて、Java ベースのクライアント アプリケーションの使用が自動的にサポートされます。
`show import webvpn plug-in`	セキュリティ アプライアンスのフラッシュ デバイスに存在するプラグインのリストを示します。

revert webvpn translation-table

セキュリティ アプライアンスのフラッシュ メモリから変換テーブルを削除するには、特権 EXEC モードで **revert webvpn translation-table** コマンドを入力します。

revert webvpn translation-table *translationdomain language*

構文の説明

translationdomain	使用可能な変換ドメインは、次のとおりです。 • AnyConnect • PortForwarder • バナー • CSD • カスタマイゼーション • URL リスト • （RDP、SSH、および VNC プラグインからのメッセージの変換）
language	削除する文字エンコーディング方法を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

インポートされた変換テーブルをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ メモリからも削除するには、**revert webvpn translation-table** コマンドを使用します。変換テーブルを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、Dutch という AnyConnect 変換テーブルを削除するコマンドを示します。

```
hostname# revert webvpn translation-table anyconnect dutch
hostname
```

関連コマンド

コマンド	説明
`revert webvpn all`	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
`show webvpn translation-table`	セキュリティ アプライアンスのフラッシュ デバイスに存在する現在の変換テーブルを表示します。

revert webvpn url-list

セキュリティ アプライアンスから URL リストを削除するには、特権 EXEC モードで **revert webvpn url-list** コマンドを入力します。

revert webvpn url-list template *name*

構文の説明

template *name*	URL リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスのフラッシュ ドライブから現在の URL リストをディセーブルにし、削除するには、**revert webvpn url-list** コマンドを使用します。URL リストを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

revert webvpn url-list コマンドで使用される template 引数では、設定済みの URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

例

次に、servers2 という URL リストを削除するコマンドを示します。

```
hostname# revert webvpn url-list servers2
hostname
```

関連コマンド

コマンド	説明
revert webvpn all	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show running-configuration url-list	現在の設定済み URL リスト コマンドのセットを表示します。
url-list（**webvpn** モード）	特定のユーザまたはグループ ポリシーに、WebVPN サーバおよび URL のリストを適用します。

revert webvpn webcontent

セキュリティ アプライアンスのフラッシュ メモリ内の場所から指定した Web オブジェクトを削除するには、特権 EXEC モードで **revert webvpn webcontent** コマンドを入力します。

revert webvpn webcontent *filename*

構文の説明

filename	削除する Web コンテンツを含むフラッシュ メモリ ファイルの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

Web コンテンツを含むファイルをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ メモリからも削除するには、**revert webvpn content** コマンドを使用します。Web コンテンツを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、セキュリティ アプライアンスのフラッシュ メモリから ABCLogo という Web コンテンツ ファイルを削除するコマンドを示します。

```
hostname# revert webvpn webcontent abclogo
hostname
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn webcontent	現在セキュリティ アプライアンスのフラッシュ メモリに存在する Web コンテンツを表示します。

revocation-check

失効チェックの 1 つ以上の方法を設定するには、クリプト CA トラストポイント モードで **revocation-check** コマンドを使用します。セキュリティ アプライアンスでは、設定した順序で各方法が試みられます。2 つめおよび 3 つめの方法は、それよりも前の順序に設定されている方法でステータスが失効として検出されず、エラーが返された場合にのみ（サーバがダウンしているなど）試みられます。

クライアント証明書検証トラストポイントで、失効チェック方法を設定できます。また、レスポンダ証明書検証トラストポイントで、失効チェックなし（**revocation-check none**）を設定することもできます。**match certificate** コマンドのマニュアルに、設定手順の例が示されています。

デフォルトの失効チェック方法（*none*）に戻すには、このコマンドの **no** 形式を使用します。

revocation-check {[**crl**] [**none**] [**ocsp**]}

no revocation-check

構文の説明

crl	セキュリティ アプライアンスにおいて、失効チェック方法として CRL を使用する必要があることを指定します。
none	セキュリティ アプライアンスにおいて、すべての方法でエラーが返された場合でも証明書ステータスを有効であると解釈する必要があることを指定します。
ocsp	セキュリティ アプライアンスにおいて、失効チェック方法として OCSP を使用する必要があることを指定します。

デフォルト

デフォルト値は *none* です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。次のように各コマンドが置き換えられました。 • **crl optional** は **revocation-check crl none** に置き換えられました。 • **crl required** は **revocation-check crl** に置き換えられました。 • **crl nocheck** は **revocation-check none** に置き換えられました。

使用上のガイドライン

OCSP 応答の署名者は、通常、OCSP サーバ（レスポンダ）証明書です。デバイスは、応答を受信した後、レスポンダ証明書の検証を試みます。

通常、CA は、セキュリティが侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は、失効ステータス チェックが必要ないことを示す ocsp-no-check 拡張をレスポンダ証明書に組み込みます。ただし、この拡張がない場合、デバイスはこの **revocation-check** コマンドでトラストポイントに設定した失効チェック方法を使用して証明書の失効ステータスのチェックを試みます。ocsp-no-check 拡張がない場合は、OCSP レスポンダ証明書は検証可能である必要があります。検証可能でないと、*none* オプションを使用してステータス チェックを無視するように設定していない限り OCSP 失効チェックに失敗するためです。

例

次に、newtrust というトラストポイントに、失効チェック方法を OCSP、CRL の順で設定する例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp crl
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。

rewrite

WebVPN 接続上で、特定のアプリケーションまたはトラフィック タイプのコンテンツのリライトをディセーブルにするには、webvpn モードで **rewrite** コマンドを使用します。リライト ルールを削除するには、ルールを一意に識別するルール番号を指定して、このコマンドの **no** 形式を使用します。すべてのリライト ルールを削除するには、このコマンドの **no** 形式をルール番号を指定せずに使用します。

デフォルトで、セキュリティ アプライアンスでは、すべての WebVPN トラフィックがリライト（変換）されます。

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

構文の説明

disable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをディセーブルにするルールとして定義します。コンテンツのリライトをディセーブルにすると、トラフィックはセキュリティ アプライアンスを通過しません。
enable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをイネーブルにするルールとして定義します。
integer	設定されているすべてのルール内でのルールの順序を設定します。指定できる範囲は 1 ～ 65534 です。
name	（任意）ルールを適用するアプリケーションまたはリソースの名前を指定します。
order	セキュリティ アプライアンスがルールを適用する順序を定義します。
resource-mask	ルールのアプリケーションまたはリソースを指定します。
resource name	（任意）ルールを適用するアプリケーションまたはリソースを指定します。最大 128 バイトです。
string	照合するアプリケーションまたはリソースの名前を指定します。正規表現を使用できます。次のワイルドカードを使用できます。 照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ?：任意の 1 文字に一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 300 バイトです。

デフォルト

デフォルトでは、すべてをリライトします。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン　セキュリティ アプライアンスでは、WebVPN 接続経由で正しくレンダリングされるように、アプリケーションのコンテンツがリライトされます。外部パブリック Web サイトなどの一部のアプリケーションでは、この処理は必要ありません。これらのアプリケーションでは、コンテンツ リライトをオフにできます。

disable オプションを指定して rewrite コマンドを使用することによって、コンテンツ リライトを選択的にオフにし、ユーザがセキュリティ アプライアンスを経由せずに直接特定のサイトをブラウズ可能にできます。これは、IPSec VPN 接続におけるスプリット トンネリングに似ています。

このコマンドは複数回使用できます。セキュリティ アプライアンスでは、順序番号に従ってリライト ルールが検索され、一致する最初のルールが適用されるため、エントリの設定順序は重要です。

例　次に、cisco.com ドメインの URL に対するコンテンツ リライトをオフにする順序番号 1 のリライト ルールを設定する例を示します。

```
hostname(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。

re-xauth

IPSec ユーザに対して IKE キー再生成時に再認証を要求するには、グループ ポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを発行します。IKE キー再生成時にユーザの再認証をディセーブルにするには、**re-xauth disable** コマンドを使用します。

実行コンフィギュレーションから re-xauth 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、他のグループ ポリシーから IKE キー再生成時の再認証についての値が継承されます。

re-xauth {**enable** [**extended**] | **disable**}

no re-xauth

構文の説明

disable	IKE キー再生成時の再認証をディセーブルにします。
enable	IKE キー再生成時の再認証をイネーブルにします。
extended	認証クレデンシャルを再入力可能な時間を、設定されている SA の最大ライフタイムまで延長します。

デフォルト

IKE キー再生成時の再認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0.4	**extended** キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IKE キー再生成時の再認証は、IPSec 接続に対してのみ適用されます。

IKE キー再生成時の再認証をイネーブルにすると、セキュリティ アプライアンスでは、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

ユーザは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。ユーザに対して、設定されている SA の最大ライフタイムまで認証クレデンシャルの再入力を許可するには、**extended** キーワードを使用します。

設定されているキー再生成間隔をチェックするには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータの KB 単位のライフタイムを表示します。

（注）　接続の他方の終端にユーザが存在しない場合、再認証は失敗します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、キー再生成時の再認証をイネーブルにする例を示します。

```
hostname(config) #group-policy FirstGroup attributes
hostname(config-group-policy)# re-xauth enable
```

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

rip send version {[**1**] [**2**]}

no rip send version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 パケットを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル RIP 送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {[**1**] [**2**]}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip authentication mode

RIP バージョン 2 パケットで使用される認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication mode** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

rip authentication mode {**text** | **md5**}

no rip authentication mode

構文の説明

md5	RIP メッセージ認証に MD5 を使用します。
text	RIP メッセージ認証にクリア テキストを使用します（非推奨）。

デフォルト

デフォルトで、クリア テキスト認証が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication key	RIP バージョン 2 認証をイネーブルにして、認証キーを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip authentication key

RIP バージョン 2 パケットの認証をイネーブルにして、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication key** コマンドを使用します。RIP バージョン 2 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

rip authentication key *key* **key_id** *key_id*

no rip authentication key

構文の説明

key	RIP 更新を認証するためのキー。このキーには、最大 16 文字を含めることができます。
key_id	キー ID 値。有効な値の範囲は 1 ～ 255 です。

デフォルト

RIP 認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。ネイバー認証をイネーブルにする場合は、*key* 引数および *key_id* 引数が、RIP バージョン 2 更新を提供するネイバー デバイスによって使用されているものと同じである必要があります。*key* は、最大 16 文字のテキスト ストリングです。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication mode	RIP バージョン 2 パケットで使用される認証のタイプを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {[**1**] [**2**]}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

rip send version {[**1**] [**2**]}

no rip send version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 パケットを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル RIP 送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0*:*	（任意）非着脱式内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）着脱式外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）取り外しできない内蔵フラッシュを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）削除するディレクトリの絶対または相対パス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ディレクトリが空でない場合、**rmdir** コマンドは失敗します。

例

次の例は、「test」という名前の既存のディレクトリを削除する方法を示しています。

```
hostname# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイル システムに関する情報を表示します。

route

指定したインターフェイスにスタティック ルートまたはデフォルト ルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定したインターフェイスからルートを削除するには、このコマンドの **no** 形式を使用します。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

構文の説明

gateway_ip	ゲートウェイ ルータの IP アドレス（このルートのネクストホップ アドレス）を指定します。 **（注）** トランスペアレント モードでは、*gateway_ip* 引数は省略可能です。
interface_name	トラフィックがルーティングされる内部または外部ネットワーク インターフェイス名。
ip_address	内部または外部ネットワーク IP アドレス。
metric	（任意）このルートのアドミニストレーティブ ディスタンス。有効値の範囲は、1 ～ 255 です。デフォルト値は、1 です
netmask	*ip_address* に適用するネットワーク マスクを指定します。
track *number*	（任意）このルートにトラッキング エントリを関連付けます。有効な値は、1 ～ 500 です。 **（注）** **track** オプションは、シングル、ルーテッド モードでのみ使用できます。
tunneled	ルートを、VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

metric のデフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	**track** *number* の値が追加されました。

使用上のガイドライン

インターフェイスに対してデフォルト ルートまたはスタティック ルートを入力するには、**route** コマンドを使用します。デフォルト ルートを入力するには、*ip_address* および *netmask* を **0.0.0.0** または短縮形の **0** に設定します。**route** コマンドを使用して入力されたすべてのルートは、コンフィギュレーションの保存時に保存されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

tunneled オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

スタティック ルートは、任意のインターフェイスで、ルータの外部に接続されているネットワークにアクセスする場合に作成します。たとえば、セキュリティ アプライアンスはこのスタティック **route** コマンドを使用して、192.168.42.0 ネットワーク宛てのすべてのパケットを、192.168.1.5 ルータ経由で送信します。

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、セキュリティ アプライアンスは、ルート テーブルに CONNECT ルートを作成します。このエントリは、**clear route** コマンドや **clear configure route** コマンドを使用しても削除されません。

route コマンドでセキュリティ アプライアンス上のいずれかのインターフェイスの IP アドレスが使用されている場合、セキュリティ アプライアンスでは、ゲートウェイ IP アドレスではなく、パケット内の宛先 IP アドレスの ARP 解決が試みられます。

例

次に、外部インターフェイスに対して、1 つのデフォルト **route** コマンドを指定する例を示します。

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

次に、ネットワークへのアクセスを提供するスタティック **route** コマンドを追加する例を示します。

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

次に、SLA 動作を使用して、外部インターフェイスに対して、10.1.1.1 ゲートウェイへのデフォルト ルートをインストールする例を示します。SLA 動作では、このゲートウェイの可用性がモニタされます。SLA 動作に失敗した場合は、dmz インターフェイスのバックアップ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
```

```
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
hostname(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

route-map

ルーティング プロトコル間でルートを再配布する条件を定義するには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

構文の説明

deny	（任意）ルート マップで一致基準が満たされると、ルートが再配布されないことを指定します。
map_tag	ルート マップ タグの最大 57 文字のテキスト。
permit	（任意）このルート マップで一致基準が満たされると、設定アクションに従ってルートが再配布されることを指定します。
seq_num	（任意）ルート マップ シーケンス番号。有効な値は、0 ～ 65535 です。同じ名前ですでに設定されているルート マップのリスト内で新しいルート マップが配置される位置を示します。

デフォルト

デフォルトの設定は次のとおりです。

- **permit**
- *seq_num* を指定しない場合は、最初のルート マップに 10 の *seq_num* が割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

route-map コマンドを使用すると、ルートを再配布できます。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドでは、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件が定義されます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは、任意の順序で入力できます。**set** コマンドによって指定された設定アクションに従ってルートが再配布されるためには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルーティング プロセス間でルートを再配布する方法を詳細に制御する必要がある場合にルート マップを使用します。宛先ルーティング プロトコルは、**router ospf** グローバル コンフィギュレーション コマンドを使用して指定します。送信元ルーティング プロトコルは、**redistribute** ルータ コンフィギュレーション コマンドを使用して指定します。

ルート マップに従ってルートを再配布する場合、複数の基準を使用してルート マップを構成できます。**route-map** コマンドに関連する少なくとも 1 つの match 句に一致しないルートは無視されます。発信ルート マップではルートはアドバタイズされず、着信ルート マップではルートは受け入れられません。一部のデータのみを変更するには、明示的な一致を指定した別のルート マップ セクションを設定する必要があります。

seq_number 引数の内容は次のとおりです。

1. 特定のタグにおいて、そのタグを指定したエントリを定義しない場合、*seq_number* 引数が 10 に設定されたエントリが作成されます。
2. 特定のタグにおいて、そのタグを指定したエントリを 1 つのみ定義した場合、そのエントリは後続の **route-map** コマンドのデフォルト エントリとなります。このエントリの *seq_number* 引数は変更されません。
3. 特定のタグにおいて、そのタグを指定したエントリを複数定義した場合は、*seq_number* 引数が必要であることを示すエラー メッセージが表示されます。

no route-map *map-tag* コマンドが（*seq-num* 引数なしで）指定されている場合、ルート マップ全体（同じ *map-tag* テキストを持つすべての **route-map** エントリ）が削除されます。

一致基準が満たされなかった場合、**permit** キーワードが指定されていると、同じ *map_tag* を持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。

例

次に、OSPF ルーティングでルート マップを設定する例を示します。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
router ospf	OSPF ルーティング プロセスを開始および設定します。

コマンド	説明
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。
show running-config route-map	ルート マップ コンフィギュレーションの情報を表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モードで **router-id** コマンドを使用します。以前のルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *addr*

no router-id [*addr*]

構文の説明

addr	IP アドレス形式でのルータ ID。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	このコマンドの処理順序が変更されました。このコマンドは、OSPF コンフィギュレーションでは、**network** コマンドよりも先に処理されるようになりました。

使用上のガイドライン

セキュリティ アプライアンスでは、OSPF コンフィギュレーションにおいて、デフォルトで、**network** コマンドによって指定されているインターフェイス上の最上位の IP アドレスが使用されます。最上位の IP アドレスがプライベート アドレスである場合、そのアドレスは hello パケットおよびデータベース定義で送信されます。特定のルータ ID を使用するには、**router-id** コマンドを使用して、ルータ ID としてグローバル アドレスを指定します。

ルータ ID は、OSPF ルーティング ドメイン内で一意である必要があります。同じ OSPF ドメイン内の 2 つのルータが同じルータ ID を使用している場合、ルーティングが正しく動作しない可能性があります。

OSPF コンフィギュレーションでは、**network** コマンドを入力する前に **router-id** コマンドを入力する必要があります。これにより、セキュリティ アプライアンスによって生成されるデフォルトのルータ ID との競合を回避できます。競合がある場合は、次のメッセージが表示されます。

```
ERROR: router-id addr in use by ospf process pid
```

競合する ID を入力するには、競合の原因となっている IP アドレスを含む **network** コマンドを削除し、**router-id** コマンドを入力して、**network** コマンドを再入力します。

例

次に、ルータ ID を 192.168.1.1 に設定する例を示します。

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

router eigrp

EIGRP ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router eigrp** コマンドを使用します。EIGRP ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

router eigrp *as-number*

no router eigrp *as-number*

構文の説明

as-number	他の EIGRP ルータへのルートを識別する自律システム番号。ルーティング情報のタギングにも使用されます。有効な値は 1 ～ 65535 です。

デフォルト

EIGRP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

router eigrp コマンドは、EIGRP ルーティング プロセスを作成するか、または既存の EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。セキュリティ アプライアンスでは、単一の EIGRP ルーティング プロセスのみを作成できます。

次のルータ コンフィギュレーション モード コマンドを使用して、EIGRP ルーティング プロセスを設定します。

- **auto-summary**：自動ルート集約をイネーブルまたはディセーブルにします。
- **default-information**：デフォルト ルート情報の送受信をイネーブルまたはディセーブルにします。
- **default-metric**：EIGRP ルーティング プロセスに再配布されるルートのデフォルトのメトリックを定義します。
- **distance eigrp**：内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定します。
- **distribute-list**：ルーティング更新で送受信されるネットワークをフィルタリングします。
- **eigrp log-neighbor-changes**：ネイバー ステートの変更のロギングをイネーブルまたはディセーブルにします。

- **eigrp log-neighbor-warnings**：ネイバー警告メッセージのロギングをイネーブルまたはディセーブルにします。
- **eigrp router-id**：固定ルータ ID を作成します。
- **eigrp stub**：セキュリティ アプライアンスでスタブ EIGRP ルーティングを設定します。
- **neighbor**：EIGRP ネイバーをスタティックに定義します。
- **network**：EIGRP ルーティング プロセスに参加するネットワークを設定します。
- **passive-interface**：パッシブ インターフェイスとして動作するインターフェイスを設定します。
- **redistribute**：他のルーティング プロセスから EIGRP にルートを再配布します。

次のインターフェイス コンフィギュレーション モード コマンドを使用して、インターフェイス固有の EIGRP パラメータを設定します。

- **authentication key eigrp**：EIGRP メッセージ認証で使用される認証キーを定義します。
- **authentication mode eigrp**：EIGRP メッセージ認証で使用される認証アルゴリズムを定義します。
- **delay**：インターフェイスの遅延メトリックを設定します。
- **hello-interval eigrp**：EIGRP の hello パケットがインターフェイスから送信される間隔を変更します。
- **hold-time eigrp**：セキュリティ アプライアンスによってアドバタイズされるホールド タイムを変更します。
- **split-horizon eigrp**：インターフェイスで EIGRP スプリット ホライズンをイネーブルまたはディセーブルにします。
- **summary-address eigrp**：サマリー アドレスを手動で定義します。

例

次に、自律システム番号 100 が付けられた EIGRP ルーティング プロセスのコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

router ospf

OSPF ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router ospf** コマンドを使用します。OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

router ospf *pid*

no router ospf *pid*

構文の説明

pid	OSPF ルーティング プロセスの内部的に使用される ID パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータの OSPF プロセスの ID と一致する必要はありません。

デフォルト

OSPF ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

router ospf コマンドは、セキュリティ アプライアンス上で実行される OSPF ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、ルータ コンフィギュレーション モードであることを示す (config-router)# コマンド プロンプトが表示されます。

no router ospf コマンドを使用する場合は、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no router ospf** コマンドは、*pid* によって指定された OSPF ルーティング プロセスを終了します。*pid* は、セキュリティ アプライアンスにおいてローカルに割り当てます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、次の OSPF 固有のコマンドとともに、OSPF ルーティング プロセスを設定するために使用されます。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：集約ルートのコスト計算に使用される方法を RFC 1583 に従った方法に戻します。
- **default-information originate**：OSPF ルーティング ドメインへのデフォルト外部ルートを生成します。

- **distance**：ルート タイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを定義します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合の syslog メッセージの送信を抑制します。
- **log-adj-changes**：OSPF ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
- **neighbor**：隣接ルータを指定します。VPN トンネル経由での隣接関係の確立を許可するために使用します。
- **network**：OSPF が実行されるインターフェイス、およびそれらのインターフェイスのエリア ID を定義します。
- **redistribute**：指定されたパラメータに従って、ルーティング ドメイン間でのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timers lsa-group-pacing**：OSPF LSA グループ ペーシング タイマー（LSA のグループがリフレッシュされる間隔または最大エージング期間に達するまでの間隔）。
- **timers spf**：SPF 計算の変更を受信するまでの遅延。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router ospf 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドをクリアします。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。

router rip

RIP ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router rip** コマンドを使用します。RIP ルーティング プロセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

router rip

no router rip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

RIP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

router rip コマンドは、セキュリティ アプライアンス上の RIP ルーティング プロセスを設定するためのグローバル コンフィギュレーション コマンドです。セキュリティ アプライアンスでは、1 つの RIP プロセスのみを設定できます。**no router rip** コマンドは、RIP ルーティング プロセスを終了し、そのプロセスのすべてのルータ コンフィギュレーションを削除します。

router rip コマンドを入力すると、コマンド プロンプトが、ルータ コンフィギュレーション モードであることを示す `hostname(config-router)#` に変更されます。

router rip コマンドは、次のルータ コンフィギュレーション コマンドとともに、RIP ルーティング プロセスを設定するために使用されます。

- **auto-summary**：ルートの自動集約をイネーブルまたはディセーブルにします。
- **default-information originate**：デフォルト ルートを配布します。
- **distribute-list in**：着信ルーティング更新のネットワークをフィルタリングします。
- **distribute-list out**：発信ルーティング更新のネットワークをフィルタリングします。
- **network**：ルーティング プロセスでインターフェイスを追加または削除します。
- **passive-interface**：特定のインターフェイスをパッシブ モードに設定します。
- **redistribute**：他のルーティング プロセスから RIP ルーティング プロセスにルートを再配布します。

- **version**：セキュリティ アプライアンスで使用される RIP プロトコル バージョンを設定します。

また、次のコマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスごとの RIP プロパティを設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 によって使用される認証のタイプを設定します。
- **rip send version**：インターフェイスから更新を送信するために使用する RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。
- **rip receive version**：インターフェイスで受け入れる RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。

トランスペアレント モードでは、RIP はサポートされていません。デフォルトで、セキュリティ アプライアンスは、すべての RIP ブロードキャスト パケットおよびマルチキャスト パケットを拒否します。これらの RIP メッセージが、トランスペアレント モードで動作するセキュリティ アプライアンスを通過できるようにするには、このトラフィックを許可するアクセス リスト エントリを定義する必要があります。たとえば、RIP バージョン 2 トラフィックがセキュリティ アプライアンスを通過することを許可するには、`access-list myriplist extended permit ip any host 224.0.0.9` のようなアクセス リスト エントリを作成します。RIP バージョン 1 ブロードキャストを許可するには、`access-list myriplist extended permit udp any any eq rip` のようなアクセス リスト エントリを作成します。**access-group** コマンドを使用して、これらのアクセス リスト エントリを適切なインターフェイスに適用します。

セキュリティ アプライアンスでは、RIP ルーティングと OSPF ルーティングの両方を同時にイネーブルにできます。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
clear configure router rip	実行コンフィギュレーションから RIP ルータ コマンドをクリアします。
show running-config router rip	実行コンフィギュレーション内の RIP ルータ コマンドを表示します。

rtp-conformance

ピンホールを通過する RTP パケットが H.323 および SIP プロトコルに準拠しているかどうかをチェックするには、パラメータ コンフィギュレーション モードで **rtp-conformance** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

構文の説明

enforce-payloadtype	シグナリング交換に基づいて、ペイロード タイプをオーディオまたはビデオであると指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ピンホールを通過する RTP パケットが H.323 コールのプロトコルに準拠しているかどうかをチェックする例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# rtp-conformance
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
debug rtp	H.323 および SIP インスペクションに関連する RTP パケットのデバッグ情報およびエラー メッセージを表示します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

CHAPTER 24

same-security-traffic コマンド～ show asdm sessions コマンド

same-security-traffic

同じセキュリティ レベルのインターフェイス間での通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可するには、グローバル コンフィギュレーション モードで **same-security-traffic** コマンドを使用します。同じセキュリティ レベルのトラフィックをディセーブルにするには、このコマンドの **no** 形式を使用します。

same-security-traffic permit {**inter-interface | intra-interface**}

no same-security-traffic permit {**inter-interface | intra-interface**}

構文の説明

inter-interface	同じセキュリティ レベルを持つ異なるインターフェイス間での通信を許可します。
intra-interface	同じインターフェイスに入って同じインターフェイスから出る通信を許可します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**intra-interface** キーワードで、IPSec トラフィックだけでなくすべてのトラフィックが、同じインターフェイスに入って同じインターフェイスから出ることが許可されるようになりました。

使用上のガイドライン

同じセキュリティ レベルのインターフェイス間での通信を許可すると（**same-security-traffic inter-interface** コマンドを使用してイネーブルにします）、次の利点があります。

- 101 より多い数の通信インターフェイスを設定できます。各インターフェイスで異なるレベルを使用する場合は、レベルごと（0 ～ 100）に 1 つのインターフェイスのみを設定できます。
- アクセス リストなしで、すべての同じセキュリティ レベルのインターフェイス間で自由にトラフィックを送受信できます。

same-security-traffic intra-interface コマンドを使用すると、トラフィックが同じインターフェイスに入って同じインターフェイスから出ることができます。この動作は、通常は許可されていません。この機能は、あるインターフェイスに入り、その後同じインターフェイスからルーティングされる VPN トラフィックの場合に役立ちます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネット

ワークがあり、セキュリティ アプライアンスがハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックはセキュリティ アプライアンスに入ってから他のスポークに再度ルーティングされる必要があります。

（注）　**same-security-traffic intra-interface** コマンドによって許可されるすべてのトラフィックには、引き続きファイアウォール ルールが適用されます。リターン トラフィックがセキュリティ アプライアンスを通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

例

次に、同じセキュリティ レベルのインターフェイス間での通信をイネーブルにする例を示します。

```
hostname(config)# same-security-traffic permit inter-interface
```

次に、トラフィックが同じインターフェイスに入って同じインターフェイスから出られるようにする例を示します。

```
hostname(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
show running-config same-security-traffic	**same-security-traffic** コンフィギュレーションを表示します。

sasl-mechanism

LDAP クライアントを LDAP サーバに対して認証するための Simple Authentication and Security Layer（SASL）メカニズムを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sasl-mechanism** コマンドを使用します。SASL 認証メカニズムのオプションは、**digest-md5** および **kerberos** です。

認証メカニズムをディセーブルにするには、このコマンドの **no** 形式を使用します。

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

（注） VPN ユーザにとっては、セキュリティ アプライアンスが LDAP サーバへのクライアント プロキシとして動作するため、ここでの LDAP クライアントとはセキュリティ アプライアンスを意味しています。

構文の説明

digest-md5	セキュリティ アプライアンスは、ユーザ名とパスワードから計算された MD5 値を使用して応答します。
kerberos	セキュリティ アプライアンスは、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信することによって応答します。
server-group-name	最大 64 文字の Kerberos AAA サーバ グループを指定します。

デフォルト

デフォルトの動作や値はありません。セキュリティ アプライアンスは、認証パラメータをプレーン テキストで LDAP サーバに渡します。

（注） SASL を設定していない場合は、**ldap-over-ssl** コマンドを使用して、SSL によって LDAP 通信を保護することを推奨します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが SASL メカニズムを使用して LDAP サーバに対する認証を行うよう指定するには、このコマンドを使用します。

セキュリティ アプライアンスと LDAP サーバの両方で、複数の SASL 認証メカニズムをサポートできます。SASL 認証をネゴシエートする場合、セキュリティ アプライアンスはサーバに設定されている SASL メカニズムのリストを取得して、セキュリティ アプライアンスとサーバの両方に設定されているメカニズムのうち最も強力な認証メカニズムを設定します。Kerberos メカニズムは、Digest-MD5 メカニズムよりも強力です。たとえば、LDAP サーバとセキュリティ アプライアンスの両方でこれら 2 つのメカニズムがサポートされている場合、セキュリティ アプライアンスでは、より強力な Kerberos メカニズムが選択されます。

各メカニズムは独立して設定されるため、SASL メカニズムをディセーブルにするには、ディセーブルにする各メカニズムに対して別々に **no** コマンドを入力する必要があります。明示的にディセーブルにしないメカニズムは引き続き有効です。たとえば、両方の SASL メカニズムをディセーブルにするには、次の両方のコマンドを入力する必要があります。

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、名前が ldapsvr1、IP アドレスが 10.10.0.1 の LDAP サーバに対する認証のために SASL メカニズムをイネーブルにする例を示します。この例では、SASL digest-md5 認証メカニズムがイネーブルにされています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
```

次に、SASL Kerberos 認証メカニズムをイネーブルにして、Kerberos AAA サーバとして kerb-servr1 を指定する例を示します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
server-type	LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

sast

CTL レコードに作成する SAST 証明書の数を指定するには、CTL ファイル コンフィギュレーション モードで **sast** コマンドを使用します。CTL ファイル内の SAST 証明書の数をデフォルト値の 2 に戻すには、このコマンドの **no** 形式を使用します。

sast *number_sasts*

no sast *number_sasts*

構文の説明

number_sasts	作成する SAST キーの数を指定します。デフォルトは 2 です。指定できる最大数は 5 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL ファイル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

CTL ファイルは、System Administrator Security Token（SAST; システム管理者セキュリティ トークン）によって署名されます。

電話プロキシは CTL ファイルを生成するため、CTL ファイル自体を署名するための SAST キーを作成する必要があります。このキーは、セキュリティ アプライアンスで生成できます。SAST は、自己署名証明書として作成されます。

通常、CTL ファイルには複数の SAST が含まれています。ある SAST が回復可能でない場合は、後でもう 1 つの SAST を使用してファイルを署名できます。

例

次に、**sast** コマンドを使用して、CTL ファイルに 5 つの SAST 証明書を作成する例を示します。

```
hostname(config-ctl-file)# sast 5
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（**Phone-Proxy**）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

secondary

フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを付与するには、フェールオーバー グループ コンフィギュレーション モードで **secondary** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

secondary

no secondary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリ プライオリティをフェールオーバー グループに割り当てることによって、両方のユニットが同時（ユニットのポーリング タイム内）に起動したときにフェールオーバー グループがアクティブになるユニットを指定します。あるユニットがもう一方のユニットよりも先にブートした場合、両方のフェールオーバー グループがそのユニットでアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
```

```
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。
primary	プライマリ ユニットに、セカンダリ ユニットよりも高いプライオリティを付与します。

secondary-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ カラーを設定するには、webvpn モードで **secondary-color** コマンドを使用します。色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-color [*color*]

no secondary-color

構文の説明

color	（任意）色を指定します。カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。 • RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。 • HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。 • 名前の最大長は 32 文字です。

デフォルト

デフォルトのセカンダリ カラーは HTML の #CCCCFF（薄紫色）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、そのうちの 40 色は MAC と PC とでは異なった表示になります。最適な結果を得るために、公開されている RGB テーブルをチェックしてください。RGB テーブルをオンラインで検索するには、検索エンジンで RGB と入力します。

例

次に、HTML の色値 #5F9EAO（灰青色）を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

関連コマンド

コマンド	説明
title-color	ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーの色を設定します。

secondary-text-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定するには、webvpn モードで **secondary-text-color** コマンドを使用します。色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-text-color [*black* | *white*]

no secondary-text-color

構文の説明

auto	text-color コマンドの設定に基づいて、黒または白が選択されます。つまり、プライマリ カラーが黒の場合、この値は白になります。
black	デフォルトのセカンダリ テキストの色は黒です。
white	テキストの色を白に変更できます。

デフォルト

デフォルトのセカンダリ テキストの色は黒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、セカンダリ テキストの色を白に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

関連コマンド

コマンド	説明
text-color	ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーのテキストの色を設定します。

secure-unit-authentication

セキュア ユニット認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **secure-unit-authentication enable** コマンドを使用します。セキュア ユニット認証をディセーブルにするには、**secure-unit-authentication disable** コマンドを使用します。実行コンフィギュレーションからセキュア ユニット認証属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにクライアントに対してユーザ名 / パスワード認証を要求することによって、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

secure-unit-authentication {**enable** | **disable**}

no secure-unit-authentication

構文の説明

disable	セキュア ユニット認証をディセーブルにします。
enable	セキュア ユニット認証をイネーブルにします。

デフォルト

セキュア ユニット認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネル グループに認証サーバ グループが設定されている必要があります。

プライマリセキュリティ アプライアンスでセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証を設定する必要があります。

例

次に、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルの場合、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットがユーザ認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

security-level

インターフェイスのセキュリティ レベルを設定するには、インターフェイス コンフィギュレーション モードで **security-level** コマンドを使用します。セキュリティ レベルをデフォルトに設定するには、このコマンドの **no** 形式を使用します。セキュリティ レベルを指定すると、高いセキュリティ レベルのネットワークと低いセキュリティ レベルのネットワークとの間の通信に追加の保護が設定され、高いセキュリティ レベルのネットワークが低いセキュリティ レベルのネットワークから保護されます。

security-level *number*

no security-level

構文の説明

number	0（最低）～ 100（最高）の整数。

デフォルト

デフォルトのセキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を指定して、明示的にセキュリティ レベルを設定しないと、セキュリティ アプライアンスによってセキュリティ レベルが 100 に設定されます（**nameif** コマンドを参照）。このレベルは必要に応じて変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**nameif** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のインスペクション エンジンは、セキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。

  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - OraServ インスペクション エンジン：ホストのペア間に OraServ ポートへの制御接続が存在する場合は、セキュリティ アプライアンス経由での着信データ接続のみが許可されます。
- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。
- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

通常、同じセキュリティ レベルのインターフェイス間では通信できません。同じセキュリティ レベルのインターフェイス間で通信する場合は、**same-security-traffic** コマンドを参照してください。101 を超える通信インターフェイスを作成する必要がある場合や、2 つのインターフェイス間のトラフィックに同じ保護機能を適用する必要がある場合（同程度のセキュリティが必要な 2 つの部門がある場合など）に、2 つのインターフェイスに同じレベルを割り当てて、それらのインターフェイス間での通信を許可できます。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

例

次に、2 つのインターフェイスのセキュリティ レベルを 100 と 0 に設定する例を示します。

```
hostname(config)# interface gigabitethernet0/0
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear local-host	すべての接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

コマンド	説明
nameif	インターフェイス名を設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

send response

RADIUS の Accounting-Response Start および Accounting-Response Stop メッセージを RADIUS の Accounting-Request Start および Stop メッセージの送信元に送信するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **send response** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスします。

このオプションは、デフォルトで無効です。

send response

no send response

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、RADIUS アカウンティングで応答を送信する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

seq-past-window

パストウィンドウ シーケンス番号（TCP 受信ウィンドウの適切な境界を越える受信 TCP パケットのシーケンス番号）を持つパケットに対するアクションを設定するには、tcp マップ コンフィギュレーション モードで **seq-past-window** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

seq-past-window {**allow** | **drop**}

no seq-past-window

構文の説明

allow	パストウィンドウ シーケンス番号を持つパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。
drop	パストウィンドウ シーケンス番号を持つパケットをドロップします。

デフォルト

デフォルトのアクションでは、パストウィンドウ シーケンス番号を持つパケットはドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **seq-past-window**：tcp マップ コンフィギュレーション モードでは、**seq-past-window** コマンドおよびその他数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、パストウィンドウ シーケンス番号を持つパケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# seq-past-window allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
queue-limit	順序が不正なパケットの制限を設定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

serial-number

登録時に、セキュリティ アプライアンスのシリアル番号を証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

serial-number

no serial-number

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定では、シリアル番号は含まれません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求にセキュリティ アプライアンスのシリアル番号を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

server

デフォルトの電子メール プロキシ サーバを指定するには、該当する電子メール プロキシ モードで **server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。セキュリティ アプライアンスは、ユーザがサーバを指定せずに電子メール プロキシに接続した場合、デフォルトの電子メール サーバに要求を送信します。デフォルトのサーバを設定せず、ユーザもサーバを指定しない場合、セキュリティ アプライアンスではエラーが返されます。

server {*ipaddr or hostname*}

no server

構文の説明

hostname	デフォルトの電子メール プロキシ サーバの DNS 名。
ipaddr	デフォルトの電子メール プロキシ サーバの IP アドレス。

デフォルト

デフォルトでは、デフォルトの電子メール プロキシ サーバはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、10.1.1.7 という IP アドレスを持つ POP3S 電子メール サーバを設定する 例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server（tls プロキシ）

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS プロキシ コンフィギュレーション モードで **server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

server trust-point *p_tp*

no server trust-point *p_tp*

構文の説明

trust-point *p_tp*	定義されているトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

TLS プロキシで TLS サーバ ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを制御するには、TLS プロキシ コンフィギュレーション モードで **server** コマンドを使用します。TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。この値は、**crypto ca trustpoint** コマンドで定義したトラストポイントに対応します。自己署名証明書、または認証局に登録された証明書を指定できます。

server コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
client	TLS プロキシで TLS クライアント ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

server authenticate-client

TLS ハンドシェイク時におけるセキュリティ アプライアンスでの TLS クライアントの認証をイネーブルにするには、TLS プロキシ コンフィギュレーション モードで **server authenticate-client** コマンドを使用します。

クライアント認証をバイパスするには、このコマンドの **no** 形式を使用します。

server authenticate-client

no server authenticate-client

構文の説明

このコマンドには、キーワードや引数はありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。つまり、セキュリティ アプライアンスとのハンドシェイク時に、TLS クライアントは、証明書の提示を要求されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TLS プロキシ ハンドシェイク時にクライアント認証が必要であるかどうかを制御するには、**server authenticate-client** コマンドを使用します。イネーブルの場合（デフォルト）、セキュリティ アプライアンスは TLS クライアントに証明書要求 TLS ハンドシェイク メッセージを送信し、TLS クライアントは証明書の提示を要求されます。

クライアント認証をディセーブルにするには、このコマンドの **no** 形式を使用します。TLS クライアント認証のディセーブルは、セキュリティ アプライアンスが CUMA クライアントや、Web ブラウザなどのクライアント証明書を送信できないクライアントと相互運用する必要がある場合に適しています。

例

次に、クライアント認証をディセーブルにした TLS プロキシ インスタンスを設定する例を示します。

```
hostname(config)# tls-proxy mmp_tls
hostname(config-tlsp)# no server authenticate-client
hostname(config-tlsp)# server trust-point cuma_server_proxy
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを設定します。

server-port

ホストの AAA サーバ ポートを設定するには、AAA サーバ ホスト モードで **server-port** コマンドを使用します。指定されているサーバ ポートを削除するには、このコマンドの **no** 形式を使用します。

server-port *port-number*

no server-port

構文の説明

port-number	0 ～ 65535 の範囲のポート番号。

デフォルト

デフォルトのサーバ ポートは次のとおりです。

- SDI：5500
- LDAP：389
- Kerberos：88
- NT：139
- TACACS+：49

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ グループ	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「srvgrp1」という名前の SDI AAA サーバでサーバ ポート番号 8888 を使用するように設定する例を示します。

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ パラメータを設定します。

clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

server-separator

電子メール サーバ名および VPN サーバ名のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **server-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの no 形式を使用します。

server-separator {*symbol*}

no server-separator

構文の説明

symbol	電子メール サーバ名および VPN サーバ名を区切る文字。選択肢は「@」（アット マーク）、「|」（パイプ）、「:（コロン）」、「#（ハッシュ）」、「,（カンマ）」、「;」（セミコロン）です。

デフォルト

デフォルトは「@」（アットマーク）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

サーバの区切り文字には、名前の区切り文字とは異なる文字を使用する必要があります。

例

次に、パイプ（|）を IMAP4S サーバの区切り文字として設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

関連コマンド

コマンド	説明
name-separator	電子メールおよび VPN のユーザ名とパスワードを区切ります。

server-type

LDAP サーバ モデルを手動で設定するには、AAA サーバ ホスト コンフィギュレーション モードで **server-type** コマンドを使用します。セキュリティ アプライアンスでは、次のサーバ モデルがサポートされています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前の Sun ONE Directory Server）
- LDAPv3 に準拠した一般的な LDAP ディレクトリ サーバ（パスワード管理なし）

このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

no server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

構文の説明

auto-detect	セキュリティ アプライアンスで自動検出によって LDAP サーバ タイプを決定することを指定します。
generic	Sun および Microsoft の LDAP ディレクトリ サーバ以外の LDAP v3 準拠のディレクトリ サーバを指定します。一般的な LDAP サーバでは、パスワード管理はサポートされません。
microsoft	LDAP サーバが Microsoft Active Directory であることを指定します。
openldap	LDAP サーバが OpenLDAP サーバであることを指定します。
novell	LDAP サーバが Novell サーバであることを指定します。
sun	LDAP サーバが Sun Microsystems JAVA System Directory Server であることを指定します。

デフォルト

デフォルトでは、自動検出によってサーバ タイプの決定が試みられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(2)	OpenLDAP および Novell サーバ タイプのサポートが追加されました。

使用上のガイドライン

セキュリティ アプライアンスは LDAP バージョン 3 をサポートしており、Sun Microsystems JAVA System Directory Server、Microsoft Active Directory、およびその他の LDAPv3 ディレクトリ サーバと互換性があります。

（注）

- Sun : Sun ディレクトリ サーバにアクセスするためにセキュリティ アプライアンスに設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft : Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- Generic : パスワード管理機能はサポートされていません。

デフォルトで、セキュリティ アプライアンスでは、Microsoft ディレクトリ サーバ、Sun LDAP ディレクトリ サーバ、または一般的な LDAPv3 サーバのいずれに接続しているかが自動検出されます。ただし、自動検出で LDAP サーバ タイプを決定できない場合で、サーバが Microsoft または Sun のサーバであることが明らかである場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバとして手動で設定できます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 のサーバ タイプを設定する例を示します。この最初の例では、Sun Microsystems LDAP サーバを設定しています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
```

次に、セキュリティ アプライアンスで自動検出を使用してサーバ タイプを決定することを指定する例を示します。

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
sasl-mechanism	LDAP クライアントおよびサーバ間での SASL 認証を設定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

server trust-point

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS サーバ コンフィギュレーション モードで **server trust-point** コマンドを使用します。

server trust-point *proxy_trustpoint*

構文の説明

proxy_trustpoint	**crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントでは、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**server trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

server trust-point コマンドは、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。証明書は、セキュリティ アプライアンス が所有している必要があります（ID 証明書）。証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。

接続を開始できる各エンティティに対して TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、TLS クライアントのロールを担います。TLS プロキシにはクライアント プロキシとサーバ プロキシが厳密に定義されているため、いずれのエンティティからも接続が開始される可能性がある場合には、2 つの TLS プロキシ インスタンスを定義する必要があります。

（注） 電話プロキシとともに使用する TLS プロキシ インスタンスを作成する場合、サーバのトラストポイントは、CTL ファイル インスタンスによって作成される内部電話プロキシ トラストポイントです。トラストポイント名は、*internal_PP_<ctl-file_instance_name>* の形式となります。

例

次に、**server trust-point** コマンドを使用して、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定する例を示します。

```
hostname(config-tlsp)# server trust-point ent_y_proxy
```

関連コマンド

コマンド	説明
client（TLS プロキシ）	TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。
client trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

service

拒否された TCP 接続のリセットをイネーブルにするには、グローバル コンフィギュレーション モードで **service** コマンドを使用します。リセットをディセーブルにするには、このコマンドの **no** 形式を使用します。

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

構文の説明

interface *interface_name*	指定したインターフェイスのリセットをイネーブルまたはディセーブルにします。
resetinbound	セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否されたすべての着信 TCP セッションに TCP リセットを送信します。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。インターフェイスを指定しない場合、この設定はすべてのインターフェイスに適用されます。
resetoutbound	セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否されたすべての発信 TCP セッションに TCP リセットを送信します。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。
resetoutside	最もセキュリティ レベルの低いインターフェイスで終端し、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否された TCP パケットのリセットをイネーブルにします。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、セキュリティ アプライアンスは拒否されたパケットを何も通知せずに廃棄します。インターフェイス PAT では、**resetoutside** キーワードを使用することを推奨します。このキーワードを使用すると、外部 SMTP または FTP サーバからの IDENT をセキュリティ アプライアンスで終了できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。

デフォルト

デフォルトで、すべてのインターフェイスで **service resetoutbound** がイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	**interface** キーワードおよび **resetoutbound** コマンドが追加されました。

使用上のガイドライン

アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセット フラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

例

次に、内部インターフェイスを除くすべてのインターフェイスで発信リセットをディセーブルにする例を示します。

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

次に、DMZ インターフェイスを除くすべてのインターフェイスで着信リセットをイネーブルにする例を示します。

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

次に、外部インターフェイスが終端となる接続でリセットをイネーブルにする例を示します。

```
hostname(config)# service resetoutside
```

関連コマンド

コマンド	説明
show running-config service	サービス コンフィギュレーションを表示します。

service（CTL プロバイダー）

証明書信頼リスト プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

service port *listening_port*

no service port *listening_port*

構文の説明

port *listening_port*	クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトのポートは 2444 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CTL プロバイダー コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。ポートは、クラスタ内の CallManager サーバによってリッスンされているポートである必要があります（[CallManager administration] ページの [Enterprise Parameters] で設定）。デフォルトのポートは 2444 です。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
client	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

service password-recovery

パスワードの回復をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。パスワードの回復をディセーブルにするには、このコマンドの **no** 形式を使用します。パスワードの回復はデフォルトでイネーブルですが、不正なユーザがパスワードの回復メカニズムを使用してセキュリティ アプライアンスを侵害できないようにするためにディセーブルにすることができます。

service password-recovery

no service password-recovery

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

パスワードの回復は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、パスワードを忘れた場合、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、ROMMON でセキュリティ アプライアンスを起動できます。次に、コンフィギュレーション レジスタを変更することによって、スタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します（**config-register** コマンドを参照）。たとえば、コンフィギュレーション レジスタがデフォルトの 0x1 の場合、**confreg 0x41** コマンドを入力して値を 0x41 に変更します。セキュリティ アプライアンスがリロードされると、デフォルトのコンフィギュレーションがロードされ、デフォルトのパスワードを使用して特権 EXEC モードを開始できます。その後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーしてスタートアップ コンフィギュレーションをロードし、パスワードをリセットします。最後に、コンフィギュレーション レジスタを元の設定に戻して、以前と同様に起動するようにセキュリティ アプライアンスを設定します。たとえば、グローバル コンフィギュレーション モードで **config-register 0x1** コマンドを入力します。

PIX 500 シリーズ セキュリティ アプライアンスでは、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、モニタ モードでセキュリティ アプライアンスを起動します。その後、PIX パスワード ツールをセキュリティ アプライアンスにダウンロードして、すべてのパスワードおよび **aaa authentication** コマンドを消去します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが ROMMON を開始することを防止でき、コンフィギュレーションも変更されないままとすることができます。ユーザが ROMMON を開始すると、ユーザは、セキュリティ アプライアンスによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、ROMMON を開始できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復は ROMMON の使用と既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。**service password-recovery** コマンドは、コンフィギュレーション ファイルに情報提供の目的でのみ表示されます。CLI プロンプトでこのコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。セキュリティ アプライアンスが起動時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワードの回復をディセーブルにすると、セキュリティ アプライアンスによって設定が変更され、通常どおりにスタートアップ コンフィギュレーションが起動されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザは、PIX パスワード ツールによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、PIX パスワード ツールを使用できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復は既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。

例

次に、ASA 5500 シリーズ適応型セキュリティ アプライアンスでパスワードの回復をディセーブルにする例を示します。

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

次に、PIX 500 シリーズ セキュリティ アプライアンスでパスワードの回復をディセーブルにする例を示します。

```
hostname(config)# no service password-recovery
WARNING: Saving "no service password-recovery" in the startup-config will disable password
recovery via the npdisk application.  The only means of recovering from lost or forgotten
passwords will be for npdisk to erase all file systems including configuration files and
images.  You should make a backup of your configuration and have a mechanism to restore
images from the Monitor Mode command line.
```

次に、ASA 5500 シリーズ適応型セキュリティ アプライアンスで、起動時に ROMMON を開始して、パスワードの回復操作を完了する例を示します。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
config-register	リロード時にスタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します。
enable password	イネーブル パスワードを設定します。
password	ログイン パスワードを設定します。

service-policy（クラス）

別のポリシー マップの下に階層型ポリシー マップを適用するには、クラス コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。階層型ポリシーは、シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを実行する場合に QoS トラフィック シェーピングでのみサポートされています。

service-policy *policymap_name*

no service-policy *policymap_name*

構文の説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。**priority** コマンドを含むレイヤ 3/4 ポリシー マップのみを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

階層型プライオリティ キューイングは、トラフィック シェーピング キューをイネーブルにするインターフェイスで使用します。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キュー（**priority-queue** コマンド）は使用しません。

階層型プライオリティ キューイングでは、Modular Policy Framework を使用して次のタスクを実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。
3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。

a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。

b. **shape**：トラフィック シェーピングをクラス マップに適用します。

c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシーマップを呼び出します。

4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	ポリシー マップにクラス マップを指定します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
policy-map	クラス マップに対して実行するアクションを指定します。
priority	プライオリティ キューイングをイネーブルにします。
service-policy（グローバル）	インターフェイスにポリシー マップを適用します。
shape	トラフィック シェーピングをイネーブルにします。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

service-policy（グローバル）

すべてのインターフェイスでグローバルに、または特定のインターフェイスでポリシー マップをアクティブにするには、グローバル コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。インターフェイスでポリシーのセットをイネーブルにするには、**service-policy** コマンドを使用します。

service-policy *policymap_name* [**global** | **interface** *intf*]

no service-policy *policymap_name* [**global** | **interface** *intf*]

構文の説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。レイヤ 3/4 ポリシー マップのみを指定できます。インスペクション ポリシー マップ（**policy-map type inspect**）は指定できません。
global	すべてのインターフェイスにポリシー マップを適用します。
interface *intf*	特定のインターフェイスにポリシー マップを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

サービス ポリシーをイネーブルにするには、Modular Policy Framework を使用します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、インスペクションのグローバル ポリシーがあり、TCP 正規化のインターフェイス ポリシーがある場合、インターフェイスに対してインスペクションと TCP 正規化の両方が適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがトラフィックにグローバルに適用されます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト サービス ポリシーには、次のコマンドが含まれています。

```
service-policy global_policy global
```

例

次に、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにする例を示します。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべてのセキュリティ アプライアンス インターフェイスで新しいポリシー new_global_policy をイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
service-policy（クラス）	別のポリシー マップの下に階層型ポリシーを適用します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

session

インテリジェント SSM（AIP SSM や CSC SSM など）への Telnet セッションを確立するには、特権 EXEC モードで **session** コマンドを使用します。

session *slot* [**do** | **ip**]

構文の説明

do	*slot* 引数で指定された SSM でコマンドを実行します。Cisco TAC によって指示された場合以外は、**do** キーワードを使用しないでください。
ip	*slot* 引数で指定された SSM のロギング IP アドレスを設定します。Cisco TAC によって指示された場合以外は、**ip** キーワードを使用しないでください。
slot	SSM スロット番号を指定します。この番号は常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**do** キーワードおよび **ip** キーワードが追加されました。これらのキーワードは、Cisco TAC によって指示された場合にのみ使用します。

使用上のガイドライン

このコマンドは、SSM がアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl-Shift-6** を押してから **X** キーを押します。

例

次に、スロット 1 の SSM へのセッションを確立する例を示します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

関連コマンド

コマンド	説明
debug session-command	セッションのデバッグ メッセージを表示します。

set connection

ポリシー マップ内のトラフィック クラスに対して接続制限を指定するには、クラス コンフィギュレーション モードで **set connection** コマンドを使用します。これらの指定を削除して、無制限の接続数を許可するには、このコマンドの **no** 形式を使用します。

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

構文の説明

conn-max *n*	許可する TCP または UDP 同時接続最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。たとえば、TCP または UDP の同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。クラスに設定された場合、このキーワードでは、クラス全体で許可される同時接続最大数が制限されます。この場合、1 つの攻撃ホストがすべての接続を使い果たし、クラスにおいてアクセス リストに一致する他のホストが使用できる接続がなくなる可能性があります。
embryonic-conn-max *n*	許可する同時初期接続最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。
per-client-embryonic-max *n*	クライアントごとに許可する同時初期接続最大数を 0 ～ 65535 の範囲で設定します。クライアントは、セキュリティ アプライアンスから（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、初期接続制限は、アクセス リストに一致するすべてのクライアントの累積初期接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。
per-client-max *n*	クライアントごとに許可する同時接続最大数を 0 ～ 65535 の範囲で設定します。クライアントは、セキュリティ アプライアンスから（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、接続制限は、アクセス リストに一致するすべてのクライアントの累積接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。クラスに設定された場合、このキーワードでは、クラスにおいてアクセス リストに一致する各ホストに許可される同時接続最大数が制限されます。
random-sequence-number {**enable** | **disable**}	TCP シーケンス番号ランダム化をイネーブルまたはディセーブルにします。このキーワードは、管理クラス マップでは使用できません。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

conn-max、**embryonic-conn-max**、**per-client-embryonic-max**、および **per-client-max** の各パラメータの *n* のデフォルト値は、0（接続数の制限なし）です。

シーケンス番号ランダム化は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**per-client-embryonic-max** キーワードおよび **per-client-max** キーワードが追加されました。
8.0(2)	このコマンドが、セキュリティ アプライアンスへの管理トラフィックにおいて、レイヤ 3/4 管理クラス マップでも使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンド（通過トラフィック）または **class-map type management** コマンド（管理トラフィック）を使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

（注） NAT コンフィギュレーションで最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定することもできます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、セキュリティ アプライアンスはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。セキュリティ アプライアンスがクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信をイネーブルにすると、3 ウェイ TCP 接続確立のハンドシェイク パケットが代行受信されるため、セキュリティ アプライアンスではクライアントレス SSL のパケットを処理できなくなります。クライアントレス SSL では、クライアントレス SSL 接続で selective-ack や他の TCP オプションを提供するために、3 ウェイ ハンドシェイク パケットを処理する機能が必要になります。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

TCP シーケンスランダム化概要

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

例

次に、**set connection** コマンドを使用して、同時接続最大数を 256 に設定し、TCP シーケンス番号ランダム化をディセーブルにする例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

次に、トラフィックを CSC SSM に転送するサービス ポリシーでの **set connection** コマンドの使用例を示します。**set connection** コマンドによって、CSC SSM でトラフィックがスキャンされる各クライアントが最大 5 接続に制限されます。

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

複数のパラメータを指定してこのコマンドを入力することも、各パラメータを個別のコマンドとして入力することもできます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが service-policy コマンドで使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシー設定を表示します。**set connection** コマンドを含むポリシーを表示するには、**set connection** キーワードを使用します。

set connection advanced-options

トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップ内で指定するには、クラス モードで **set connection advanced-options** コマンドを使用します。トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップから削除するには、クラス モードで、このコマンドの **no** 形式を使用します。

set connection advanced-options *tcp-mapname*

no set connection advanced-options *tcp-mapname*

構文の説明

tcp-mapname	高度な TCP 接続オプションの設定対象となる TCP マップの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行するには、TCP マップ名に加えて、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。詳細については、**tcp-map** コマンドの説明を参照してください。

例

次に、**set connection advanced-options** コマンドを使用して、localmap という名前の TCP マップの使用を指定する例を示します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
class-map	クラス マップ モードで match コマンドを 1 つだけ（tunnel-group および default-inspection-traffic を除く）発行し、一致基準を指定することによって、トラフィック クラスを設定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

set connection decrement-ttl

ポリシー マップ内のトラフィック クラスにおいて存続可能時間の値をデクリメントするには、クラス コンフィギュレーション モードで **set connection decrement-ttl** コマンドを使用します。存続可能時間をデクリメントしない場合は、このコマンドの **no** 形式を使用します。

set connection decrement-ttl

no set connection decrement-ttl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトで、セキュリティ アプライアンスでは、存続可能時間はデクリメントされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンド、および **icmp unreachable** コマンドは、セキュリティ アプライアンスをホップの 1 つとして表示するセキュリティ アプライアンス経由の traceroute を可能とするために必要です。

例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが **service-policy** コマンドで使用されている場合、そのポリシー マップは削除されません。
icmp unreachable	ICMP 到達不能メッセージがセキュリティ アプライアンスを通過可能なレートを制御します。

policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
show service-policy	サービス ポリシー設定を表示します。

set connection timeout

ポリシー マップ内のトラフィック クラスに対して接続タイムアウトを指定するには、クラス コンフィギュレーション モードで **set connection timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

構文の説明

dcd	Dead Connection Detection（DCD; デッド接続検出）をイネーブルにします。DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。TCP 接続がタイムアウトすると、セキュリティ アプライアンスは、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、セキュリティ アプライアンスはその接続を解放します。両方のエンドホストが応答して接続の有効性が確認されると、セキュリティ アプライアンスはアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。
embryonic *hh*:*mm*:*ss*	TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間を 0:0:5 ～ 1193:0:0 の範囲で設定します。デフォルトは 0:0:30 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。初期接続とは、スリーウェイ ハンドシェイクが完了していない TCP 接続です。
half-closed *hh*:*mm*:*ss*	ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間を 0:5:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 0:10:0 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。ハーフクローズの接続は DCD の影響を受けません。また、セキュリティ アプライアンスは、ハーフクローズ接続を切断するときにリセット パケットを送信しません。
max_retries	DCD において、何回連続して再試行に失敗すると接続がデッドであると見なされるかを設定します。最小値は 1、最大値は 255 です。デフォルトは 5 です。
reset	TCP のアイドル接続が削除されてから、両方のエンド システムに TCP RST パケットを送信します。
retry_interval	DCD プローブに応答がない場合に次のプローブを送信するまでの *hh*:*mm*:*ss* 形式の間隔を 0:0:1 ～ 24:0:0 の範囲で指定します。デフォルトは 0:0:15 です。
tcp *hh*:*mm*:*ss*	確立された接続が終了するアイドル タイムアウト時間を設定します。

デフォルト

デフォルトの **embryonic** タイムアウトは 30 秒です。

デフォルトの **half-closed** アイドル タイムアウトは 10 分です。

デフォルトの **dcd** *max_retries* の値は 5 です。

デフォルトの **dcd** *retry_interval* の値は 15 秒です。

デフォルトの **tcp** アイドル タイムアウトは 1 時間です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DCD のサポートが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンドを使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection timeout** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

DCD をイネーブルにすると、TCP ノーマライザでのアイドルタイムアウト処理の動作が変更されます。DCD プローブにより、**show conn** コマンドで表示される接続でのアイドル タイムアウトがリセットされます。タイムアウト コマンドで設定したタイムアウト値を超過していても、DCD プローブのために存続している接続を判別するため、**show service-policy** コマンドには、DCD からのアクティビティ数を示すカウンタが含まれています。

例

次に、すべてのトラフィックの接続タイムアウトを設定する例を示します。

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection timeout tcp 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection timeout embryonic 0:40:0
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続の値を設定します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
show service-policy	DCD およびその他のサービス アクティビティのカウンタを表示します。

set metric

ルーティング プロトコルのメトリック値を設定するには、ルート マップ コンフィギュレーション モードで **metric** コマンドを使用します。デフォルトのメトリック値に戻すには、このコマンドの **no** 形式を使用します。

set metric *value*

no set metric *value*

構文の説明

value	メトリック値。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

no set metric *value* コマンドを使用すると、デフォルトのメトリック値に戻すことができます。このコンテキストでは、*value* は 0 ～ 4294967295 の整数です。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。

set metric-type

OSPF メトリック ルートのタイプを指定するには、ルート マップ コンフィギュレーション モードで **set metric-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set metric-type {**type-1** | **type-2**}

no set metric-type

構文の説明

type-1	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。
type-2	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。

デフォルト

デフォルトは、**type-2** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルート マップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# set metric-type type-2
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

setup

対話形式のプロンプトを使用してセキュリティ アプライアンスの最小限度のコンフィギュレーションを設定するには、グローバル コンフィギュレーション モードで **setup** コマンドを入力します。このコンフィギュレーションでは、ASDM を使用するための接続が提供されます。デフォルトのコンフィギュレーションに戻すには、**configure factory-default** コマンドも参照してください。

setup

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

フラッシュ メモリにスタートアップ コンフィギュレーションがない場合は、起動時に設定ダイアログ ボックスが自動的に表示されます。

setup コマンドを使用する前に、内部インターフェイスを設定しておく必要があります。PIX 500 シリーズのデフォルト コンフィギュレーションには内部インターフェイス（イーサネット 1）が含まれていますが、ASA 550 シリーズのデフォルト コンフィギュレーションには含まれていません。**setup** コマンドを使用する前に、内部インターフェイスにするインターフェイスに対して **interface** コマンドを入力して、**nameif inside** コマンドを入力します。

マルチ コンテキスト モードでは、システム実行スペースおよび各コンテキストに対して **setup** コマンドを使用できます。

setup コマンドを入力すると、表 24-1 の情報の入力を求められます。システムの **setup** コマンドには、これらのプロンプトのサブセットが含まれています。プロンプトに表示されたパラメータのコンフィギュレーションがすでに存在する場合は、そのコンフィギュレーションが角カッコに表示されます。その値をデフォルトとして受け入れるか、または新しい値を入力してその値を上書きできます。

表 24-1　設定プロンプト

プロンプト	説明
Pre-configure Firewall now through interactive prompts [yes]?	**yes** または **no** を入力します。**yes** を入力すると、設定ダイアログボックスが続行します。**no** を入力すると、設定ダイアログボックスが停止し、グローバル コンフィギュレーション プロンプト（hostname(config)#）が表示されます。
Firewall Mode [Routed]:	**routed** または **transparent** を入力します。
Enable password:	イネーブル パスワードを入力します （パスワードは、3 文字以上である必要があります)。
Allow password recovery [yes]?	**yes** または **no** を入力します。
Clock (UTC):	このフィールドには何も入力できません。デフォルトで UTC 時間が使用されます。
Year:	4 桁の年（2005 など）を入力します。年の範囲は 1993 ～ 2035 です。
Month:	月の先頭の 3 文字（9 月の場合は **Sep** など）を使用して月を入力します。
Day:	日付（1 ～ 31）を入力します。
Time:	24 時間制で時間、分、秒を入力します。たとえば、午後 8 時 54 分 44 秒の場合は、**20:54:44** と入力します。
Inside IP address:	内部インターフェイスの IP アドレスを入力します。
Inside network mask:	内部 IP アドレスに適用するネットワーク マスクを入力します。255.0.0.0 や 255.255.0.0 などの有効なネットワーク マスクを指定する必要があります。
Host name:	コマンドライン プロンプトに表示するホスト名を入力します。
Domain name:	セキュリティ アプライアンスを稼働するネットワークのドメイン名を入力します。
IP address of host running Device Manager:	ASDM にアクセスする必要があるホストの IP アドレスを入力します。
Use this configuration and write to flash?	**yes** または **no** を入力します。**yes** を入力すると、内部インターフェイスがイネーブルになり、要求されたコンフィギュレーションがフラッシュ パーティションに書き込まれます。 **no** を入力すると、設定ダイアログボックスが最初の質問から繰り返されます。 `Pre-configure Firewall now through interactive prompts [yes]?` 設定ダイアログボックスを終了するには **no** を、設定ダイアログボックスを繰り返すには **yes** を入力します。

例

次に、**setup** コマンド プロンプトを完了する例を示します。

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
```

```
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

関連コマンド

コマンド	説明
configure factory-default	デフォルトのコンフィギュレーションに戻します。

shape

QoS トラフィック シェーピングをイネーブルにするには、クラス コンフィギュレーション モードで **shape** コマンドを使用します。セキュリティ アプライアンスなどの、ファスト イーサネットを使用してパケットを高速に送信するデバイスが存在し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、ケーブル モデムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされます。さまざまな回線速度を持つネットワークを管理するために、低い固定レートでパケットを送信するようにセキュリティ アプライアンスを設定できます。これを *トラフィック シェーピング*と呼びます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

構文の説明

average *rate*	一定期間におけるトラフィックの平均レート（ビット/秒）を 64000 ～ 154400000 の範囲で設定します。8000 の倍数の値を指定します。期間の計算方法の詳細については、「使用上のガイドライン」の項を参照してください。
burst_size	一定期間において送信可能な平均バースト サイズ（ビット単位）を 2048 ～ 154400000 の範囲で設定します。128 の倍数の値を指定します。*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

デフォルト

burst_size を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

トラフィック シェーピングをイネーブルにするには、Modular Policy Framework を使用します。

1. **policy-map**：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。

b. **shape**：トラフィック シェーピングをクラス マップに適用します。

c. （任意）**service-policy**：シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを適用できるように、**priority** コマンドを設定した異なるポリシー マップを呼び出します。

2. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

トラフィック シェーピングの概要

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延の原因になる可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。

- トラフィック シェーピングは、物理インターフェイスのすべての発信トラフィック、または ASA 5505 の場合は VLAN 上のすべての発信トラフィックに適用する必要があります。特定のタイプのトラフィックにはトラフィック シェーピングを設定できません。
- トラフィック シェーピングはインターフェイス上でパケットの送信準備が完了したときに適用されるため、レート計算は、IPSec ヘッダーや L2 ヘッダーなどのすべてのオーバーヘッドを含む、実際の送信パケット サイズに基づいて行われます。
- シェーピングされるトラフィックには、through-the-box トラフィックと from-the-box トラフィックの両方が含まれます。
- シェープ レートの計算は、標準トークン バケット アルゴリズムに基づいて行われます。トークン バケット サイズは、バースト サイズ値の 2 倍です。トークン バケットの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
- バースト性のトラフィックが指定されたシェープ レートを超えると、パケットはキューに入れられて、後で送信されます。次に、シェーピング キューのいくつかの特性について説明します（階層型プライオリティ キューイングの詳細については、**priority** コマンドを参照してください）。
  - キューのサイズは、シェープ レートに基づいて計算されます。キューは、1500 バイトのパケットとして 200 ミリ秒に相当するシェープ レート トラフィックを保持できます。最小キュー サイズは 64 です。
  - キューの制限に達すると、パケットはキューの末尾からドロップされます。
  - OSPF Hello パケットなどの一部の重要なキープアライブ パケットは、ドロップされません。
  - 時間間隔は、*time_interval* = *burst_size* / *average_rate* によって求められます。時間間隔が長くなるほど、シェープ トラフィックのバースト性は高くなり、リンクのアイドル状態が長くなる可能性があります。この効果は、次のような誇張した例を使うとよく理解できます。

    平均レート = 1000000

    バースト サイズ = 1000000

    この例では、時間間隔は 1 秒であり、これは、100 Mbps の FE リンクでは 1 Mbps のトラフィックを時間間隔 1 秒の最初の 10 ミリ秒内にバースト送信できることを意味し、残りの 990 ミリ秒間はアイドル状態になって、次の時間間隔になるまでパケットを送信できません。したがって、音声トラフィックのように遅延が問題になるトラフィックがある場合は、バースト サイズを平均レートと比較して小さくし、時間間隔を短くする必要があります。

QoS 機能の相互作用のしくみ

セキュリティ アプライアンスで必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能をセキュリティ アプライアンスに設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。たとえば、グローバル ポリシーに標準プライオリティ キューイングを設定して、特定のインターフェイスにトラフィック シェーピングを設定する場合、最後に設定した機能は拒否されます。これは、グローバル ポリシーがインターフェイス ポリシーと重複するためです。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定はセキュリティ アプライアンスでは制限されていません。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップ内でアクションを実行するクラス マップを指定します。
police	QoS ポリシングをイネーブルにします。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
priority	QoS プライオリティ キューイングをイネーブルにします。
service-policy（クラス）	階層型ポリシー マップを適用します。
service-policy（グローバル）	サービス ポリシーをインターフェイスに適用します。
show service-policy	QoS 統計情報を表示します。

show aaa local user

現在ロックされているユーザ名のリストを表示するか、またはユーザ名の詳細を表示するには、グローバル コンフィギュレーション モードで **aaa local user** コマンドを使用します。

show aaa local user [**locked**]

構文の説明

locked	（任意）現在ロックされているユーザ名のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションのキーワード **locked** を省略すると、セキュリティ アプライアンスによって、すべての AAA ローカル ユーザの失敗試行およびロックアウト ステータスの詳細が表示されます。

username オプションを使用して単一のユーザを指定するか、**all** オプションを使用してすべてのユーザを指定できます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響します。

管理者をデバイスからロックアウトすることはできません。

例

次に、**show aaa local user** コマンドを使用して、すべてのユーザ名のロックアウト ステータスを表示する例を示します。

次に、制限を 5 回に設定した後に **show aaa local user** コマンドを使用して、すべての AAA ローカル ユーザの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

次に、制限を 5 回に設定した後に **lockout** キーワードを指定して **show aaa local user** コマンドを使用し、ロックアウトされている AAA ローカル ユーザのみの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザが何回誤ったパスワードを入力するとロック アウトされるかを示す最大回数を設定します。
clear aaa local user fail-attempts	ロックアウト ステータスを変更しないで、失敗試行回数を 0 にリセットします。
clear aaa local user lockout	指定したユーザまたはすべてのユーザのロックアウト ステータスをクリアして、それらのユーザの失敗試行カウンタを 0 に設定します。

show aaa-server

AAA サーバの AAA サーバ統計情報を表示するには、特権 EXEC モードで **show aaa-server** コマンドを使用します。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

LOCAL	（任意）ローカル ユーザ データベースの統計情報を表示します。
groupname	（任意）グループ内のサーバの統計情報を表示します。
host *hostname*	（任意）グループ内の特定のサーバの統計情報を表示します。
protocol *protocol*	（任意）指定したプロトコルのサーバの統計情報を表示します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトで、すべての AAA サーバ統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	http-form プロトコルが追加されました。
8.0(2)	**aaa-server active** コマンドまたは **fail** コマンドを使用して手動でステータスが変更されたかどうかがサーバ ステータスに表示されるようになりました。

例

次に、**show aaa-server** コマンドを使用して、サーバ グループ group1 の特定のホストの統計情報を表示する例を示します。

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
```

```
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

次に、**show aaa-server** コマンドのフィールド説明を示します。

フィールド	説明
Server Group	**aaa-server** コマンドによって指定されたサーバ グループ名。
Server Protocol	**aaa-server** コマンドによって指定されたサーバ グループのサーバ プロトコル。
Server Address	AAA サーバの IP アドレス。
Server port	セキュリティ アプライアンスおよび AAA サーバによって使用される通信ポート。RADIUS 認証ポートは、**authentication-port** コマンドを使用して指定できます。RADIUS アカウンティング ポートは、**accounting-port** コマンドを使用して指定できます。非 RADIUS サーバでは、ポートは **server-port** コマンドによって設定されます。
Server status	サーバのステータス。次のいずれかの値が表示されます。 • ACTIVE : セキュリティ アプライアンスはこの AAA サーバと通信します。 • FAILED : セキュリティ アプライアンスはこの AAA サーバと通信できません。この状態になったサーバは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。 ステータスの後に「(admin initiated)」と表示されている場合、このサーバは、**aaa-server active** コマンドまたは **fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。 また、次の形式で最終トランザクションの日時も表示されます。 **Last transaction (**{**success** | **failure**}**) at** *time timezone date* セキュリティ アプライアンスがサーバと通信したことがない場合は、次のメッセージが表示されます。 **Last transaction at Unknown**
Number of pending requests	現在進行中の要求数。
Average round trip time	サーバとのトランザクションを完了するまでにかかる平均時間。
Number of authentication requests	セキュリティ アプライアンスによって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。

フィールド	説明
Number of authorization requests	認可要求数。この値は、コマンド認可、through-the-box トラフィックの認可（TACACS+ サーバ）、またはトンネル グループに対してイネーブルにされた WebVPN および IPSec 認可機能による認可要求を指しています。この値には、タイムアウト後の再送信は含まれていません。
Number of accounting requests	アカウンティング要求数。この値には、タイムアウト後の再送信は含まれていません。
Number of retransmissions	内部タイムアウト後にメッセージが再送信された回数。この値は、Kerberos および RADIUS サーバ（UDP）にのみ適用されます。
Number of accepts	成功した認証要求数。
Number of rejects	拒否された要求数。この値には、エラー状態、および実際にクレデンシャルが AAA サーバから拒否された場合の両方が含まれます。
Number of challenges	最初にユーザ名とパスワードの情報を受信した後に、AAA サーバがユーザに対して追加の情報を要求した回数。
Number of malformed responses	該当なし。将来的な使用のために予約されています。
Number of bad authenticators	次のいずれかが発生した回数。 • RADIUS パケットの「authenticator」ストリングが破損している（まれなケース）。 • セキュリティ アプライアンスの共有秘密キーと RADIUS サーバの共有秘密キーが一致しない。この問題を修正するには、適切なサーバ キーを入力します。 この値は、RADIUS にのみ適用されます。
Number of timeouts	セキュリティ アプライアンスが、AAA サーバが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。
Number of unrecognized responses	認識できない応答またはサポートしていない応答をセキュリティ アプライアンスが AAA サーバから受信した回数。たとえば、サーバからの RADIUS パケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」、または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバからの RADIUS 応答パケットが破損していることを意味していますが、まれなケースです。

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバ グループ内のすべてのサーバ、または特定のサーバの統計情報を表示します。
clear aaa-server statistics	AAA サーバ統計情報をクリアします。

show access-list

アクセス リストのカウンタを表示するには、特権 EXEC モードで **show access-list** コマンドを使用します。

show access-list *id_1* [...[*id_2*]] [**brief**]

構文の説明

acl_name_1	既存のアクセス リストを識別する名前または文字セット。
acl_name_2	既存のアクセス リストを識別する名前または文字セット。
brief	アクセス リスト識別子およびヒット カウントを 16 進数形式で表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	**brief** キーワードのサポートが追加されました。

使用上のガイドライン

1 つのコマンドに複数のアクセス リスト識別子を入力することによって、一度に複数のアクセス リストを表示できます。

brief キーワードを指定して、16 進数形式でアクセス リスト ヒット カウントおよび識別子情報を表示できます。16 進数形式で表示されるコンフィギュレーション識別子は 2 列に表示され、syslog 106023 および 106100 で使用される識別子と同じです。

例

次に、**show access-list** コマンドの出力例を示します。

```
hostname# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
             alert-interval 300
access-list 101; 10 elements
access-list 101 line 1 extended permit tcp any eq www any (hitcnt=0) 0xa14fc533
access-list 101 line 2 extended permit tcp any eq www any eq www (hitcnt=0) 0xaa73834e
access-list 101 line 3 extended permit tcp any eq www any range telnet www (hitcnt=0)
0x49ac02e6
access-list 101 line 4 extended permit tcp any range telnet www any range telnet www
(hitcnt=0) 0xa0021a9f
access-list 101 line 5 extended permit udp any range biff www any (hitcnt=0) 0xf89a7328
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43 access-list
101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
```

```
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

この出力では、各行の最後に個々のアクセス コントロール エントリに対する独自の 16 進数の識別子が含まれています。

次に、**show access-list brief** コマンドの出力例を示します。

```
hostname (config)# sh access-list abc brief

abc:
28676dfa 00000000 00000001
bbec063f f0109e02 000000a1
3afd0576 f0109e02 000000c2
a83ddc02 f0109e02 00000021
hostname (config)#
```

最初の 2 列に識別子が 16 進数形式で表示され、3 列めにヒット カウントが 16 進数形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。ヒット カウントがゼロの場合、情報は表示されません。

関連コマンド

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show activation-key

実行アクティベーション キー、および許可されているコンテキスト数を含む、アクティベーション キーによってイネーブルにされているコンフィギュレーション内のライセンス済み機能を表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。

show activation-key [detail]

（注）　このコマンドは、PIX プラットフォームではサポートされません。

構文の説明

detail キーワードを使用すると、永久アクティベーション キーと一時アクティベーション キーおよびこれらのキーによってイネーブルにされる機能が表示されます（以前にインストールされたすべての一時キーおよびこれらのキーの有効期限を含む）。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(4)	**detail** キーワードが追加されました。

使用上のガイドライン

show activation-key コマンド出力では、次のようにアクティベーション キーのステータスが表示されます。

- セキュリティ アプライアンス のフラッシュ ファイル システム内のアクティベーション キーがセキュリティ アプライアンスで実行されているアクティベーション キーと同じである場合、**show activation-key** の出力は次のようになります。

```
The flash activation key is the SAME as the running key.
```

- セキュリティ アプライアンス のフラッシュ ファイル システムのアクティベーション キーとセキュリティ アプライアンスで稼働するアクティベーション キーが異なる場合、**show activation-key** の出力は次のようになります。

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- アクティベーション キーをダウングレードすると、動作中のキー（古いキー）とフラッシュに格納されているキー（新しいキー）が異なることを示す出力が表示されます。セキュリティ アプライアンス を再起動すると、新しいキーが使用されます。
- アクティベーション キーをアップグレードして、追加の機能をイネーブルにした場合は、再起動しなくても新しいキーがただちに動作を開始します。
- PIX Firewall プラットフォームでは、新しいキーと古いキーの間でフェールオーバー機能（R/UR/FO）に変更があった場合、確認が求められます。**n** を入力すると、変更が中止されます。それ以外の場合は、フラッシュ ファイル システムのキーが更新されます。セキュリティ アプライアンス を再起動すると、新しいキーが使用されます。
- 以前のリリースにダウングレードした場合、現在のリリースのキーでは、以前のリリースでサポートされている数よりも多くのセキュリティ コンテキストが使用できる場合があります。キーのセキュリティ コンテキストの値がプラットフォームの制限を超えると、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: 50 security contexts exceeds the limit in the
  platform, reduce to 20 security contexts.
  ```

- 以前のリリースにダウングレードした場合、現在のリリースのキーでは GTP/GPRS がイネーブルであるにもかかわらず、以前のリリースでは GTP/GPRS が許可されていないことがあります。キーを使用して GTP/GPRS をイネーブルにしても、GTP/GPRS がソフトウェアのバージョンによって許可されない場合は、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
  GTP/GPRS.
  ```

一時アクティベーション キーは時間ベースのアクティベーション キーであり、このキーは、**activation-key** コマンドを使用して有効または無効にできます。一時アクティベーション キーを無効にすると、永久アクティベーション キーを割り当てることができます。永久アクティベーション キーは、非時間ベースのアクティベーション キーです。一時アクティベーション キーは、後で再度アクティブにできるので削除できません。

一時アクティベーション キーと永久アクティベーション キーは、両方ともフラッシュ ファイル システムに保管されます。適用されるキーは、機能しているアクティベーション キーです。一時アクティベーション キーは、一度に 1 つだけ適用できます。一時アクティベーション キーがすでに適用されているセキュリティ アプライアンスに一時アクティベーション キーを適用すると、古い一時アクティベーション キーは無効になり、新しい一時アクティベーション キーが適用されます。

セキュリティ アプライアンスは、アクティブになっているすべての一時アクティベーション キーを追跡します。一時アクティベーション キーが失効すると、セキュリティ アプライアンスにより、失効したことが通知されます。一時アクティベーション キーは、失効すると表示されなくなります。アクティブでない一時アクティベーション キーは、別の一時アクティベーション キーまたは永久アクティベーション キーによって適用され、上書きされたキーです。

例

次に、コンフィギュレーション内のコマンドのうち、アクティベーション キーでイネーブルにされた機能に関するものを表示する例を示します。

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada
The Running Activation Key feature: 50 security contexts exceeds the limit in the
platform, reduce to 20 security contexts.
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
GTP/GPRS.

License Features for this Platform:
Maximum Physical Interfaces : Unlimited
```

```
Maximum VLANs               : 50
Inside Hosts                : Unlimited
Failover                    : Enabled
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL-filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
VPN Peers                   : 5000
Advanced Endpoint Assessment: Disabled
UC Proxy Sessions            : 2

The flash activation key is the SAME as the running key.
```

次の例は、一時アクティベーション キーおよび永久アクティベーション キーによってイネーブルになったコンフィギュレーションに含まれているライセンス付き機能を表示する方法を示しています。

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
Permanent Flash Activation Key: 0x31245147 0x3834b49a 0x98b391b4
0x95b83030 0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

Temporary Flash Activation Key: 0x051e96ff 0x98937617 0x79cbe717
0x502449e7 0x862b92ab

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Disabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
WebVPN Peers                 : 2
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions            : 2
This is a time-based license that will expire in 27 day(s).
```

次の例は、永久アクティベーション キーによってイネーブルになったコンフィギュレーションに含まれているライセンス付き機能を表示する方法を示しています。

```
hostname(config)# show activation-key detail
```

```
Serial Number:  JMX0916L0Z4
No active temporary key.
Running Activation Key: 0x31245147 0x3834b49a 0x98b391b4 0x95b83030
0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

This platform has an ASA 5540 VPN Premium license.

The flash activation key is the SAME as the running key.

Non-active temporary keys:                                Time left
-----------------------------------------------------------------------
0x2a53d6   0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2  28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397  27 day(s
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを変更します。

show ad-groups

Active Directory サーバにリストされているグループを表示するには、特権 EXEC モードで **show ad-groups** コマンドを使用します。

show ad-groups *name* [**filter** *string*]

構文の説明

name	問い合わせる Active Directory サーバ グループの名前。
string	検索するグループ名の全体または一部を指定する、引用符で囲んだ問い合わせに含めるストリング。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

show ad-groups コマンドは、グループの取得に LDAP プロトコルを使用する Active Directory サーバに対してのみ適用されます。このコマンドを使用して、ダイナミック アクセス ポリシー AAA 選択基準に使用できる AD グループを表示します。

LDAP 属性タイプが LDAP の場合、セキュリティ アプライアンスがサーバからの応答を待機するデフォルト時間は 10 秒です。この時間は、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用して調整できます。

（注） Active Directory サーバに数多くのグループが含まれている場合は、サーバが応答パケットに格納できるデータ量の制限に基づいて **show ad-groups** コマンドの出力が切り捨てられることがあります。この問題を回避するには、**filter** オプションを使用して、サーバからレポートされるグループ数を減らします。

例

```
hostname# show ad-groups LDAP-AD17
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

次に、同じコマンドで **filter** オプションを使用した例を示します。

```
hostname(config)# show ad-groups LDAP-AD17 filter “Eng”
.
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
group-search-timeout	グループのリストについて Active Directory サーバからの応答をセキュリティ アプライアンスが待機する時間を調整します。

show admin-context

現在管理コンテキストとして割り当てられているコンテキスト名を表示するには、特権 EXEC モードで **show admin-context** コマンドを使用します。

show admin-context

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show admin-context** コマンドの出力例を示します。次の例では、「admin」という名前で、フラッシュのルート ディレクトリに保存されている管理コンテキストが表示されています。

```
hostname# show admin-context
Admin: admin flash:/admin.cfg
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
clear configure context	すべてのコンテキストを削除します。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

show arp

ARP テーブルを表示するには、特権 EXEC モードで **show arp** コマンドを使用します。

show arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	表示にダイナミック ARP エージングが追加されました。

使用上のガイドライン

表示出力には、ダイナミック、スタティック、およびプロキシ ARP エントリが表示されます。ダイナミック ARP エントリには、ARP エントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARP エントリにはダッシュ（-）が、プロキシ ARP エントリには「alias」という状態が含まれています。

例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
hostname# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、特権 EXEC モードで **show arp-inspection** コマンドを使用します。

show arp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show arp-inspection** コマンドの出力例を示します。

```
hostname# show arp-inspection
interface                arp-inspection         miss
-----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp statistics

ARP 統計情報を表示するには、特権 EXEC モードで show arp statistics コマンドを使用します。

show arp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show arp statistics** コマンドの出力例を示します。

```
hostname# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 2 に、各フィールドの説明を示します。

表 24-2　show arp statistics のフィールド

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。
Maximum queued blocks	IP アドレスの解決を待機している間に ARP モジュールにキューイングされた最大ブロック数。
Queued blocks	現在 ARP モジュールにキューイングされているブロック数。

表 24-2　show arp statistics のフィールド （続き）

フィールド	説明
Interface collision ARPs received	セキュリティ アプライアンスのインターフェイスと同じ IP アドレスからの ARP パケットがセキュリティ アプライアンスのすべてのインターフェイスで受信されたパケット数。
ARP-defense gratuitous ARPs sent	ARP-Defense メカニズムの一環としてセキュリティ アプライアンスによって送信された Gratuitous ARP の数。
Total ARP retries	最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。
Unresolved hosts	現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。
Maximum unresolved hosts	最後にクリアされた後、またはセキュリティ アプライアンスの起動後に、ARP モジュールに存在した未解決ホストの最大数。

関連コマンド

コマンド	説明
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアして、値をゼロにリセットします。
show arp	ARP テーブルを表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show asdm history

ASDM 履歴バッファの内容を表示するには、特権 EXEC モードで **show asdm history** コマンドを使用します。

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

構文の説明

asdmclient	（任意）ASDM クライアント用にフォーマットされた ASDM 履歴データを表示します。
feature *feature*	（任意）履歴表示を指定した機能に制限します。*feature* 引数には、次の値を指定できます。 • **all**：すべての機能の履歴を表示します（デフォルト）。 • **blocks**：システム バッファの履歴を表示します。 • **cpu**：CPU 使用状況の履歴を表示します。 • **failover**：フェールオーバーの履歴を表示します。 • **ids**：IDS の履歴を表示します。 • **interface** *if_name*：指定したインターフェイスの履歴を表示します。*if_name* 引数は、**nameif** コマンドで指定したインターフェイスの名前です。 • **memory**：メモリ使用状況の履歴を表示します。 • **perfmon**：パフォーマンス履歴を表示します。 • **sas**：セキュリティ アソシエーションの履歴を表示します。 • **tunnels**：トンネルの履歴を表示します。 • **xlates**：変換スロット履歴を表示します。
snapshot	（任意）最後の ASDM 履歴データ ポイントのみを表示します。
view *timeframe*	（任意）履歴の表示を指定した期間に制限します。*timeframe* 引数には、次の値を指定できます。 • **all**：履歴バッファ内のすべての内容（デフォルト）。 • **12h**：12 時間 • **5d**：5 日 • **60m**：60 分 • **10m**：10 分

デフォルト

引数またはキーワードを指定しない場合は、すべての機能のすべての履歴情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm history** コマンドから **show asdm history** コマンドに変更されました。

使用上のガイドライン

show asdm history コマンドは、ASDM 履歴バッファの内容を表示します。ASDM 履歴情報を表示する前に、**asdm history enable** コマンドを使用して、ASDM 履歴トラッキングをイネーブルにする必要があります。

例

次に、**show asdm history** コマンドの出力例を示します。このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。

```
hostname# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
```

```
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

次に、**show asdm history** コマンドの出力例を示します。前の例と同様に、このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。ただし、この例では、出力は ASDM クライアント用にフォーマットされています。

```
hostname# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|
25026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|
25102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|
25169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|
25381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750|
750|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|751|751|
751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753|753|
753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|
55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|
55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|
4381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|
5401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698|
5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349|
5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|3349|
5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|
5|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|
7|6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
```

```
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|
375010|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|
375395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|
375794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|
376200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
hostname#
```

次に、**snapshot** キーワードを使用した **show asdm history** コマンドの出力例を示します。

```
hostname# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
```

```
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
```

```
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
```

```
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
hostname#
```

関連コマンド

コマンド	説明
asdm history enable	ASDM 履歴トラッキングをイネーブルにします。

show asdm image

現在の ASDM ソフトウェア イメージ ファイルを表示するには、特権 EXEC モードで **show asdm image** コマンドを使用します。

show asdm image

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm image** コマンドから **show asdm image** コマンドに変更されました。

例

次に、**show asdm image** コマンドの出力例を示します。

```
hostname# show asdm image

Device Manager image file, flash:/ASDM
```

関連コマンド

コマンド	説明
asdm image	現在の ASDM イメージ ファイルを指定します。

show asdm log_sessions

アクティブな ASDM ロギング セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm log_sessions** コマンドを使用します。

show asdm log_sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから Syslog メッセージを取得します。各 ASDM ロギング セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect log_session** コマンドで使用して、指定したセッションを終了できます。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギング セッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

例

次に、**show asdm log_sessions** コマンドの出力例を示します。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect log_session	アクティブな ASDM ロギング セッションを終了します。

show asdm sessions

アクティブな ASDM セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm sessions** コマンドを使用します。

show asdm sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm sessions** コマンドから **show asdm sessions** コマンドに変更されました。

使用上のガイドライン

アクティブな各 ASDM セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect** コマンドで使用して、指定したセッションを終了できます。

例

次に、**show asdm sessions** コマンドの出力例を示します。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect	アクティブな ASDM セッションを終了します。

CHAPTER 25

show asp drop コマンド～ show curpriv コマンド

show asp drop

高速セキュリティ パスでドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

構文の説明

flow [*flow_drop_reason*]	（任意）ドロップされたフロー（接続）を表示します。*flow_drop_reason* 引数を使用して、特定の理由を指定できます。*flow_drop_reason* 引数の有効な値は、下記の「使用上のガイドライン」に示されています。
frame [*frame_drop_reason*]	（任意）ドロップされたパケットを表示します。*frame_drop_reason* 引数を使用して、特定の理由を指定できます。*frame_drop_reason* 引数の有効な値は、下記の「使用上のガイドライン」に示されています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.0(8)/7.2(4)/8.0(4)	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれるようになりました（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理由のキーワードが表示されるため、そのキーワードを使用して簡単に **capture asp-drop** コマンドを使用できます。

使用上のガイドライン

show asp drop コマンドは、高速セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

次の項では、各ドロップ理由の名前、説明、および推奨事項を示します。

- 「フレームのドロップ理由」（P.25-2）
- 「フローのドロップ理由」（P.25-38）

フレームのドロップ理由

```
Name: punt-rate-limit
Punt rate limit exceeded:
    This counter will increment when the appliance attempts to forward a layer-2 packet to
a rate-limited control point service routine and the rate limit (per/second) is now being
exceeded. Currently, the only layer-2 packets destined for a control point service routine
which are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second
per interface.

Recommendation:
    Analyze your network traffic to determine the reason behind the high rate of ARP
packets.

 Syslogs:
    322002, 322003


----------------------------------------------------------------
Name: invalid-encap
Invalid Encapsulation:
    This counter is incremented when the security appliance receives a frame belonging to
an unsupported link-level protocol or if the L3type specified in the frame is not
supported by the appliance. The packet is dropped.

Recommendation:
    Verify that directly connected hosts have proper link-level protocol settings.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-header
Invalid IP header:
    This counter is incremented and the packet is dropped when the appliance receives an
IP packet whose computed checksum of the IP header does not match the recorded checksum in
the header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a peer is sending corrupted packets and an attack is in progress. Please use the
packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: unsupported-ip-version
Unsupported IP version:
    This counter is incremented when the security appliance receives an IP packet that has
an unsupported version in version field of IP header. Specifically, if the packet does not
belong to version 4 or version 6. The packet is dropped.

Recommendation:
    Verify that other devices on connected network are configured to send IP packets
belonging to versions 4 or 6 only.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-length
Invalid IP Length:
```

```
    This counter is incremented when the security appliance receives an IPv4 or IPv6
packet in which the header length or total length fields in IP header are not valid or do
not conform to the received packet length.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ethertype
Invalid Ethertype:
    This counter is incremented when the fragmentation module on the security appliance
receives or tries to send a fragmented packet that does not belong IP version 4 or version
6. The packet is dropped.

Recommendation:
    Verify mtu of device and other devices on connected network to  determine why the
device is processing such fragments.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-tcp-hdr-length
Invalid TCP Length:
    This counter is incremented when the security appliance receives a TCP packet whose
size is smaller than minimum-allowed header length or does not conform to the received
packet length.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.
Investigate the traffic from source in the following syslog.
Syslogs:
    500003.


----------------------------------------------------------------
Name: invalid-udp-length
Invalid UDP Length:
    This counter is incremented when the security appliance receives a UDP packet whose
size as calculated from the fields in header is different from the measured size of packet
as received from the network.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter is incremented when the security appliance has tried to obtian an
adjacency and could not obtain mac-address for next hop. The packet is dropped.

Recommendation:
    Configure a capture for this drop reason and check if a host with specified
destination address exists on connected network or is routable from the device.
```

```
Syslogs:
   None.


----------------------------------------------------------------
Name: unexpected-packet
Unexpected packet:
    This counter is incremented when the appliance in transparent mode receives a non-IP
packet, destined to it's MAC address, but there is no corresponding service running on the
appliance to process the packet.

Recommendation:
    Verify if the appliance is under attack. If there are no suspicious packets, or the
device is not in transparent mode, this counter is most likely being incremented due to a
software error. Attempt to capture the traffic that is causing the counter to increment
and contact the Cisco TAC.

Syslogs:
    None


----------------------------------------------------------------
Name: no-route
No route to host:
    This counter is incremented when the security appliance tries to send a packet out of
an interface and does not find a route for it in routing table.

Recommendation:
    Verify that a route exists for the destination address obtained from thegenerated
syslog.

Syslogs:
   110001.


----------------------------------------------------------------
Name: rpf-violated
Reverse-path verify failed:
    This counter is incremented when ip-verify is configured on an interface and the
security appliance receives a packet for which the route lookup of source-ip did not yield
the same interface as the one on which the packet was received.

Recommendation:
    Trace the source of traffic based on source-ip printed in syslog below and investigate
why it is sending spoofed traffic.

Syslogs:
    106021.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by configured rule:
    This counter is incremented when a drop rule is hit by the packet and gets dropped.
This rule could be a default rule created when the box comes up, when various features are
turned on or off, when an acl is applied to interface or any other feature etc. Apart from
default rule drops, a packet could be dropped because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface

Recommendation:
    Note if one of ACLs listed below are fired.
```

```
Syslogs:
    106023, 106100, 106004


----------------------------------------------------------------
Name: unable-to-create-flow
Flow denied due to resource limitation:
    This counter is incremented and the packet is dropped when flow creation fails due to
a system resource limitation.  The resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
    Causes 1 and 2 will occur simultaneously with flow drop reason "No memory to complete
flow".

Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with the command
"show resource usage".

Syslogs:
    None


----------------------------------------------------------------
Name: unable-to-add-flow
Flow hash full:
    This counter is incremented when a newly created flow is inserted into flow hash table
and the insertion failed because the hash table was full. The flow and the packet are
dropped. This is different from counter that gets incremented when maximum connection
limit is reached.

Recommendation:
    This message signifies lack of resources on the device to support an operation that
should have been successful. Please check if the connections in the 'show conn' output
have exceeded their configured idle timeout values. If so, contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None.


----------------------------------------------------------------
Name: np-sp-invalid-spi
Invalid SPI:
    This counter will increment when the appliance receives an IPSec ESP packet addressed
to the appliance which specifies a SPI (security parameter index) not currently known by
the appliance.

 Recommendation:
    Occasional invalid SPI indications are common, especially during rekey processing.
Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing
a high rate of invalid SPI indications, analyze your network traffic to determine the
source of the ESP traffic.

 Syslogs:
    402114


----------------------------------------------------------------
Name: unsupport-ipv6-hdr
Unsupported IPv6 header:
```

```
    This counter is incremented and the packet is dropped if an IPv6 packet is received
with an unsupported IPv6 extension header.  The supported IPv6 extension headers are: TCP,
UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment.  The IPv6 routing
extension header is not supported, and any extension header not listed above is not
supported.  IPv6 ESP and AH headers are supported only if the packet is through-the-box.
To-the-box IPv6 ESP and AH packets are not supported and will be dropped.

Recommendation:
    This error may be due to a misconfigured host.  If this error occurs repeatedly or in
large numbers, it could also indicate spurious or malicious activity such as an attempted
DoS attack.
Syslogs:
    None.


----------------------------------------------------------------
Name: natt-keepalive
NAT-T keepalive message:
    This counter will increment when the appliance receives an IPSec NAT-T keepalive
message.  NAT-T keepalive messages are sent from the IPSec peer to the appliance to keep
NAT/PAT flow information current in network devices between the NAT-T IPSec peer and the
appliance.

 Recommendation:
    If you have configured IPSec NAT-T on your appliance, this indication is normal and
doesn't indicate a problem.  If NAT-T is not configured on your appliance, analyze your
network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: tcp-not-syn
First TCP packet not SYN:
    Received a non SYN packet as the first packet of a non intercepted and non nailed
connection.

Recommendation:
    Under normal conditions, this may be seen when the appliance has already closed a
connection, and the client or server still believe the connection is open, and continue to
transmit data.  Some examples where this may occur is just after a 'clear local-host' or
'clear xlate' is issued. Also, if connections have not been recently removed, and the
counter is incrementing rapidly, the appliance may be under attack. Capture a sniffer
trace to help isolate the cause.
Syslogs:
    6106015


----------------------------------------------------------------
Name: bad-tcp-cksum
Bad TCP checksum:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow
packets with incorrect TCP checksum disable checksum-verification feature under tcp-map.

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: bad-tcp-flags
Bad TCP flags:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with invalid TCP flags in TCP header. Example a packet with SYN and FIN TCP
flags set will be dropped.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-reserved-set
TCP reserved flags set:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with reserved flags set in TCP header.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow such
TCP packets or clear reserved flags and then pass the packet use reserved-bits
configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-bad-option-list
TCP option list invalid:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with a non-standard TCP header option.

Recommendations:
    To allow such TCP packets or clear non-standard TCP header options and then allow the
packet, use tcp-options configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-mss-exceeded
TCP data exceeded MSS:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with data length greater than the MSS advertized by peer TCP endpoint.

Recommendations:
    To allow such TCP packets use exceed-mss configuration under tcp-map

Syslogs:
    4419001


----------------------------------------------------------------
Name: tcp-synack-data
TCP SYNACK with data:
```

```
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN-ACK packet with data.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-syn-data
TCP SYN with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet with data.

Recommendations:
    To allow such TCP packets use syn-data configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dual-open
TCP Dual open denied:
    This counter is incremented and the packet is dropped when the appliance recevies a
TCP SYN packet from the server, when an embryonic TCP connection is already open.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-data-past-fin
TCP data send after FIN:
    This counter is incremented and the packet is dropped when the appliance recevies new
TCP data packet from an endpoint which had sent a FIN to close the connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-3whs-failed
TCP failed 3 way handshake:
    This counter is incremented and the packet is dropped when appliance receives an
invalid TCP packet during three-way-handshake. Example SYN-ACK from client will be dropped
for this reason.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-rstfin-ooo
TCP RST/FIN out of order:
    This counter is incremented and the packet is dropped when appliance receives a RST or
a FIN packet with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-seq-syn-diff
TCP SEQ in SYN/SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a SYN or
SYN-ACK packet during three-way-handshake with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-ack-syn-diff
TCP ACK in SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a
SYN-ACK packet during three-way-handshake with incorrect TCP acknowledgement number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-syn-ooo
TCP SYN on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-synack-ooo
TCP SYNACK on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN-ACK packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-seq-past-win
TCP packet SEQ past window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
data packet with sequence number beyond the window allowed by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-invalid-ack
TCP invalid ACK:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with acknowledgement number greater than data sent by peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-fo-drop
TCP replicated flow pak drop:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with control flag like SYN, FIN or RST on an established connection just after the
appliance has taken over as active unit.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-discarded-ooo
TCP ACK in 3 way handshake invalid:
    This counter is incremented and the packet is dropped when appliance receives a TCP
ACK packet from client during three-way-handshake and the sequence number is not next
expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-full
TCP Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when appliance receives an
out-of-order TCP packet on a connection and there is no buffer space to store this packet.
Typically TCP packets are put into order on connections that are inspected by the
appliance or when packets are sent to SSM for inspection. There is a default queue size
and when packets in excess of this default queue size are received they will be dropped.
```

```
Recommendations:
    On ASA platforms the queue size could be increased using queue-limit configuration
under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-global-buffer-full
TCP global Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when the security appliance
receives an out-of-order TCP packet on a connection and there are no more global buffers
available. Typically TCP packets are put into order on connections that are inspected by
the security appliance or when packets are sent to the SSM for inspection. When the global
Out-of-Order buffer queue is full, the packet will be dropped and this counter will
increment.

Recommendations:
    This is a temporary condition when all global buffers are used. If this counter is
constantly incrementing, then please check your network for large amounts of Out-of-Order
traffic, which could be caused by traffic of the same flow taking different routes through
the network.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-timeout
TCP Out-of-Order packet buffer timeout:
    This counter is incremented and the packet is dropped when a queued out of order TCP
packet has been held in the buffer for too long.Typically, TCP packets are put into order
on connections that are inspected by the security appliance or when packets are sent to
the SSM for inspection. When the next expected TCP packet does not arrive within a certain
period, the queued out of order packet is dropped.

Recommendations:
    The next expected TCP packet may not arrive due to congestion in the network which is
normal in a busy network. The TCP retransmission mechanism in the end host will retransmit
the packet and the session will continue.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-rst-syn-in-win
TCP RST/SYN in window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN or TCP RST packet on an established connection with sequence number within window but
not next expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-acked
TCP DUP and has been ACKed:
```

```
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet and the data has been acknowledged by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dup-in-queue
TCP dup of packet in Out-of-Order queue:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet that is already in our out of order packet queue.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-paws-fail
TCP packet failed PAWS test:
    This counter is incremented and the packet is dropped when TCP packet with timestamp
header option fails the PAWS (Protect Against Wrapped Sequences) test.

Recommendations:
    To allow such connections to proceed, use tcp-options configuration under tcp-map to
clear timestamp option.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-conn-limit
TCP connection limit reached:
    This reason is given for dropping a TCP packet during TCP connection establishment
phase when the connection limit has been exceeded.  The connection limit is configured via
the 'set connection conn-max' action command.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached.  The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: conn-limit
Connection limit reached:
    This reason is given for dropping a packet when the connection limit or host
connection limit has been exceeded.  If this is a TCP packet which is dropped during TCP
connection establishment phase due to connection limit, the drop reason 'TCP connection
limit reached' is also reported.

Recommendation:
```

```
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached.  The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp_xmit_partial
TCP retransmission partial:
    This counter is incremented and the packet is dropped when check-retranmission feature
is enabled and a partial TCP retransmission was received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This counter is incremented and the packet is dropped when check-retranmission feature
is enabled and a TCP retranmission with different data from the original packet was
received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This counter is incremented and the packet is dropped when window size advertized by
TCP endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow such packet, use the window-variation configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: ipsecudp-keepalive
IPSEC/UDP keepalive message:
    This counter will increment when the appliance receives an IPSec over UDP keepalive
message. IPSec over UDP keepalive messages are sent from the IPSec peer to the appliance
to keep NAT/PAT flow information current in network devices between the IPSec over UDP
peer and the appliance. Note - These are not industry standard NAT-T keepalive messages
which are also carried over UDP and addressed to UDP port 4500.
 Recommendation:
    If you have configured IPSec over UDP on your appliance, this indication is normal and
doesn't indicate a problem.  If IPSec over UDP is not configured on your appliance,
analyze your network traffic to determine the source of the IPSec over UDP traffic.

 Syslogs:
    None
```

```
----------------------------------------------------------------
Name: rate-exceeded
QoS rate exceeded:
    This counter is incremented when rate-limiting (policing) is configured on an
egress/ingress interface and the egress/ingress traffic rate exceeds the burst rate
configured. The counter is incremented for each packet dropped.

Recommendation:
    Investigate and determine why the rate of traffic leaving/entering the interface is
higher than the configured rate. This may be normal, or could be an indication of virus or
attempted attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: queue-removed
Rate-limiter queued packet dropped:
    When QoS config is changed or removed, the existing packets in the output queues
awaiting transmission are dropped and this counter is incremented.

Recommendation:
    Under normal conditions, this may be seen when the QoS configuration has been changed
by the user. If this occurs when no changes to QoS config were performed, please contact
Cisco Technical Assistance Center (TAC).

Syslogs:
   None.


----------------------------------------------------------------
Name: bad-crypto
Bad crypto return in packet:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors.  You can also check the error counter in the global IPSec statistics with
the 'show ipsec stats' CLI command. If the IPSec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: bad-ipsec-prot
IPSec not AH or ESP:
    This counter will increment when the appliance receives a packet on an IPSec
connection which is not an AH or ESP protocol. This is not a normal condition.

 Recommendation:
    If you are receiving many IPSec not AH or ESP indications on your appliance, analyze
your network traffic to determine the source of the traffic.

 Syslogs:
    402115
```

```
----------------------------------------------------------------
Name: ipsec-ipv6
IPSec via IPV6:
    This counter will increment when the appliance receives an IPSec ESP packet, IPSec
NAT-T ESP packet or an IPSec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPSec sessions encapsulated in IP version 6.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-natt
BAD IPSec NATT packet:
    This counter will increment when the appliance receives a packet on an IPSec
connection which has negotiated NAT-T but the packet is not addressed to the NAT-T UDP
destination port of 4500 or had an invalid payload length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-udp
BAD IPSec UDP packet:
    This counter will increment when the appliance receives a packet on an IPSec
connection which has negotiated IPSec over UDP but the packet has an invalid payload
length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-need-sa
IPSec SA not negotiated yet:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPSec security association. This is generally a normal
condition for LAN-to-LAN IPSec configurations. This indication will cause the appliance to
begin ISAKMP negotiations with the destination peer.

 Recommendation:
    If you have configured IPSec LAN-to-LAN on your appliance, this indication is normal
and doesn't indicate a problem.  However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing. Verify that you can communicate with the destination peer and verify your
crypto configuration via the 'show running-config' command.

 Syslogs:
    None


----------------------------------------------------------------
Name: ctm-error
```

```
CTM returned error:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance.

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors.  You can also check the error counter in the global IPSec statistics with
the 'show ipsec stats' CLI command. If the IPSec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be     useful
in diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: send-ctm-error
Send to CTM returned error:
    This counter is obsolete in the appliance and should never increment.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof
IPSec spoof detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.  The packet matched the inner header security policy check of
a configured and established IPSec connection on the appliance but was received
unencrypted.  This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-clearpkt-notun
IPSec Clear Pkt w/no tunnel:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.  The packet matched the inner header security policy check of
a configured and established IPSec connection on the appliance but was received
unencrypted.  This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-tun-down
IPSec tunnel is down:
    This counter will increment when the appliance receives a packet associated with an
IPSec connection which is in the process of being deleted.
```

```
 Recommendation:
    This is a normal condition when the IPSec tunnel is torn down for any reason.

 Syslogs:
    None


----------------------------------------------------------------
Name: security-failed
Early security checks failed:
    This counter is incremented and packet is dropped when the security appliance :
    - receives an IPv4 multicast packet when the packets multicast MAC address doesn't
match the packets multicast destination IP address
    - receives an IPv6 or IPv4 teardrop fragment containing either small offset or
fragment overlapping
    - receives an IPv4 packet that matches an IP audit (IPS) signature

Recommendation:
    Contact the remote peer administrator or escalate this issue according to your
security policy
    For detailed description and syslogs for IP audit attack checks please refer the ip
audit signature section of command reference guide

Syslogs:
    106020
    400xx in case of ip audit checks


----------------------------------------------------------------
Name: sp-security-failed
Slowpath security checks failed:
    This counter is incremented and packet is dropped when the security appliance is:
    1) In routed mode receives a through-the-box:
       - L2 broadcast packet
       - IPv4 packet with destination IP address equal to 0.0.0.0
       - IPv4 packet with source IP address equal to 0.0.0.0
    2) In routed or transparent mode and receives a through-the-box IPv4 packet with:
       - first octet of the source IP address equal to zero
       - source IP address equal to the loopback IP address
       - network part of source IP address equal to all 0's
       - network part of the source IP address equal to all 1's
       - source IP address host part equal to all 0's or all 1's
    3) In routed or transparent mode and receives an IPv4 or IPv6 packet with same source
and destination IP addresses

Recommendation:
    1 and 2) Determine if an external user is trying to compromise the protected network.
Check for misconfigured clients.
    3) If this message counter is incrementing rapidly, an attack may be in progress. Use
the packet capture feature to capture type asp packets, and check the source MAC address
in the packet to see where they are coming from.

Syslogs:
    1 and 2) 106016
    3) 106017


----------------------------------------------------------------
Name: ipv6_sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
```

```
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.  Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.
Syslogs:
    For identical source and destination address, syslog 106016, else none.


----------------------------------------------------------------
Name: invalid-ip-option
IP option drop:
    This counter is incremented when any unicast packet with ip options or a multicast
packet with ip-options that have not been configured to be accepted, is received by the
security appliance. The packet is dropped.

Recommendation:
    Investigate why a packet with ip options is being sent by the sender.

Syslogs:
    None.


----------------------------------------------------------------
Name: lu-invalid-pkt
Invalid LU packet:
    Standby unit received a corrupted Logical Update packet.

Recommendation:
    The packet corruption could be caused by a bad cable, interface card, line noise, or
software defect. If the interface appears to be functioning properly, then report the
problem to Cisco TAC.

Syslogs:
    None


----------------------------------------------------------------
Name: fo-standby
Dropped by standby unit:
    If a through-the-box packet arrives at an appliance or context in a Standby state and
a flow is created, the packet is dropped and the flow removed. This counter will increment
each time a packet is dropped in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: dst-l2_lookup-fail
Dst MAC L2 Lookup Failed:
    This counter will increment when the appliance is configured for transparent mode and
the appliance does a Layer 2 destination MAC address lookup which fails.  Upon the lookup
failure, the appliance will begin the destination MAC discovery process and attempt to
find the location of the host via ARP and/or ICMP messages.

 Recommendation:
```

```
    This is a normal condition when the appliance is configured for transparent mode. You
can also execute (show mac-address-table) to list the L2 MAC address locations currently
discovered by the appliance.

 Syslogs:
    None


----------------------------------------------------------------
Name: l2_same-lan-port
L2 Src/Dst same LAN port:
    This counter will increment when the appliance/context is configured for transparent
mode and the appliance determines that the destination interface's L2 MAC address is the
same as its ingress interface.

 Recommendation:
    This is a normal condition when the appliance/context is configured for transparent
mode.  Since the appliance interface is operating in promiscuous mode, the
appliance/context receives all packets on the local LAN seqment.

 Syslogs:
    None


----------------------------------------------------------------
Name: flow-expired
Expired flow:
    This counter is incremented when the security appliance tries to inject a new or
cached packet belonging to a flow that has already expired.It is also incremented when the
appliance attempts to send an rst on a tcp flow that has already expired or when a packet
returns from IDS blade but the flow had already expired. The packet is dropped

Recommendation:
    If valid applications are getting pre-empted, investigate if a longer timeout is
needed.

Syslogs:
   None.


----------------------------------------------------------------
Name: inspect-icmp-out-of-app-id
ICMP Inspect out of App ID:
    This counter will increment when the ICMP inspection engine fails to allocate an 'App
ID' data structure.  The structure is used to store the sequence number of the ICMP
packet.

Recommendation:
    Check the system memory usage.  This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmp-seq-num-not-matched
ICMP Inspect seq num not matched:
    This counter will increment when the sequence number in the ICMP echo reply message
does not match any ICMP echo message that passed across the appliance earlier on the same
connection.

Recommendation:
```

```
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004


----------------------------------------------------------------
Name: inspect-icmp-error-no-existing-conn
ICMP Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMP error message.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-different-embedded-conn
ICMP Error Inspect different embedded conn:
    This counter will increment when the frame embedded in the ICMP error message does not
match the established connection that has been identified when the ICMP connection is
created.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmpv6-error-invalid-pak
ICMPv6 Error Inspect invalid packet:
    This counter will increment when the appliance detects an invalid frame embedded in
the ICMPv6 packet.  This check is the same as that on IPv6 packets. Examples: Incomplete
IPv6 header; malformed IPv6 Next Header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmpv6-error-no-existing-conn
ICMPv6 Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMPv6 error message.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005
```

```
----------------------------------------------------------------
Name: inspect-dns-invalid-pak
DNS Inspect invalid packet:
    This counter will increment when the appliance detects an invalid DNS packet.
Examples: A DNS packet with no DNS header; the number of DNS resource records not matching
the counter in the header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-invalid-domain-label
DNS Inspect invalid domain label:
    This counter will increment when the appliance detects an invalid DNS domain name or
label. DNS domain name and label is checked per RFC 1035.

Recommendation:
    No action required.  If the domain name and label check is not desired, disable the
protocol-enforcement parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-pak-too-long
DNS Inspect packet too long:
    This counter is incremented when the length of the DNS message exceeds the configured
maximum allowed value.

Recommendation:
    No action required.  If DNS message length checking is not desired, enable DNS
inspection without the 'maximum-length' option, or disable the 'message-length maximum'
parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    410001


----------------------------------------------------------------
Name: inspect-dns-out-of-app-id
DNS Inspect out of App ID:
    This counter will increment when the DNS inspection engine fails to allocate a data
structure to store the identification of the DNS message.
Recommendation:
    Check the system memory usage.  This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-id-not-matched
DNS Inspect ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.

Recommendation:
```

```
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: dns-guard-out-of-app-id
DNS Guard out of App ID:
    This counter will increment when the DNS Guard function fails to allocate a data
structure to store the identification of the DNS message.

Recommendation:
    Check the system memory usage.  This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: dns-guard-id-not-matched
DNS Guard ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.
This counter will increment by the DNS Guard function.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-length
Invalid RTP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTP header.

Recommendation:
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-version
Invalid RTP Version field:
    This counter will increment when the RTP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTP packets conformant with
the RFC 1889. The reason for this has to be identified and you can deny the host using
ACLs if required.

Syslogs:
    431001.
```

```
----------------------------------------------------------------
Name: inspect-rtp-invalid-payload-type
Invalid RTP Payload type field:
    This counter will increment when the RTP payload type field does not contain an audio
payload type when the signalling channel negotiated an audio media type for this RTP
secondary connection. The counter increments similarly for the video payload type.

Recommendation:
    The RTP source in your network is using the audio RTP secondary connection to send
video  or vice versa. If you wish to prevent this you can deny the host using ACLs.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-ssrc-mismatch
Invalid RTP Synchronization Source field:
    This counter will increment when the RTP SSRC field in the packet does not match the
SSRC which the inspect has been seeing from this RTP source in all the RTP packets.

Recommendation:
    This could be because the RTP source in your network is rebooting and hence changing
the SSRC or it could be because of another host on your network trying to use the opened
secondary RTP connections on the firewall to send RTP packets. This should be investigated
further to confirm if there is a problem.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-sequence-num-outofrange
RTP Sequence number out of range:
    This counter will increment when the RTP sequence number in the packet is not in the
range expected by the inspect.

Recommendation:
    No action is required because the inspect tries to recover and start tracking from a
new sequence number after a lapse in the sequence numbers from the RTP source.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-max-outofseq-paks-probation
RTP out of sequence packets in probation period:
    This counter will increment when the out of sequence packets when the RTP source is
being validated exceeds 20. During the probation period, the inspect looks for 5
in-sequence packets to consider the source validated.

Recommendation:
    Check the RTP source to see why the first few packets do not come in sequence and
correct it.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-length
Invalid RTCP Packet length:
```

```
    This counter will increment when the UDP packet length is less than the size of the
RTCP header.

Recommendation:
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-version
Invalid RTCP Version field:
    This counter will increment when the RTCP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTCP packets conformant
with the RFC 1889. The reason for this has to be identified and you can deny the host
using ACLs if required.

Syslogs:
    431002.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-payload-type
Invalid RTCP Payload type field:
    This counter will increment when the RTCP payload type field does not contain the
values 200 to 204.

Recommendation:
    The RTP source should be validated to see why it is sending payload types outside of
the range recommended by the RFC 1889.

Syslogs:
    431002.


----------------------------------------------------------------
Name: inspect-srtp-encrypt-failed
Inspect SRTP Encryption failed:
    This counter will increment when SRTP encryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP encryption is
failing in the hardware crypto accelerator.

Syslogs:
    337001.


----------------------------------------------------------------
Name: inspect-srtp-decrypt-failed
Inspect SRTP Decryption failed:
    This counter will increment when SRTP decryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP decryption is
failing in the hardware crypto accelerator.

Syslogs:
    337002.
```

```
----------------------------------------------------------------
Name: inspect-srtp-validate-authtag-failed
Inspect SRTP Authentication tag validation failed:
    This counter will increment when SRTP authentication tag validation fails.

Recommendation:
    No action is required. If error persists SRTP packets arriving at the firewall are
being tampered with and the administrator has to identify the cause.

Syslogs:
    337003.


----------------------------------------------------------------
Name: inspect-srtp-generate-authtag-failed
Inspect SRTP Authentication tag generation failed:
    This counter will increment when SRTP authentication tag generation fails.

Recommendation:
    No action is required.

Syslogs:
    337004.


----------------------------------------------------------------
Name: inspect-srtp-no-output-flow
Inspect SRTP failed to find output flow:
    This counter will increment when the flow from the Phone proxy could not be created or
if the flow has been torn down

Recommendation:
    No action is required. The flow creation could have failed because of low memory
conditions.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-setup-srtp-failed
Inspect SRTP setup in CTM failed:
    This counter will increment when SRTP setup in the CTM fails.

Recommendation:
    No action is required. If error persists call TAC to see why the CTM calls are
failing.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-one-part-no-key
Inspect SRTP failed to find keys for both parties:
    This counter will increment when Inspect SRTP finds only one party's keys populated in
the media session.

Recommendation:
    No action is required. This counter could increment in the beginning phase of the call
but eventually when the call signaling exchange completes both parties should know their
respective keys.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-media-session
Inspect SRTP Media session lookup failed:
    This counter will increment when SRTP media session lookup fails.

Recommendation:
    No action is required. The media session is created by Inspect SIP or Skinny when the
IP address is parsed as part of the signaling exchange. Debug the signaling messages to
figure out the cause.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-remote-phone-proxy-ip
Inspect SRTP Remote Phone Proxy IP not populated:
    This counter will increment when remote phone proxy IP is not populated

Recommendation:
    No action is required. The remote phone proxy IP address is populated from the
signaling exchange. If error persists debug the signaling messages to figure out if ASA is
seeing all the signaling messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-client-port-not-present
Inspect SRTP client port wildcarded in media session:
    This counter will increment when client port is not populated in media session

Recommendation:
    No action is required. The client port is populated dynamically when the media stream
comes in from the client. Capture the media packets to see if the client is sending media
packets.

Syslogs:
    None.


----------------------------------------------------------------
Name: ips-request
IPS Module requested drop:
    This counter is incremented and the packet is dropped as requested by IPS module when
the packet matches a signature on the IPS engine.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: ips-fail-close
IPS card is down:
```

```
    This counter is incremented and the packet is dropped when IPS card is down and
fail-close option was used in IPS inspection.

Recommendations:
    Check and bring up the IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: ips-fail
IPS config removed for connection:
    This counter is incremented and the packet is dropped when IPS configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for IPS.

Syslogs:
   None


----------------------------------------------------------------
Name: l2_acl
FP L2 rule drop:
    This counter will increment when the appliance denies a packet due to a layer-2 ACL.
By default, in routed mode the appliance will PERMIT:
    1) IPv4 packets
    2) IPv6 packets
    3) ARP packets
    4) L2 Destination MAC of FFFF:FFFF:FFFF (broadcast)
    5) IPv4 MCAST packet with destination L2 of 0100:5E00:0000-0100:5EFE:FFFF
    6) IPv6 MCAST packet with destination L2 of 3333:0000:0000-3333:FFFF:FFFF

    By default, in Transparent mode permits the routed mode ACL and PERMITS:

    1) BPDU packets with destination L2 of 0100:0CCC:CCCD
    2) Appletalk packets with destination L2 of 0900:0700:0000-0900:07FF:FFFF

    The user can also configure ethertype ACL(s) and apply them to an interface to permit
other types of L2 traffic.

    Note - Packets permitted by L2 ACLs may still be dropped by L3-L4 ACLs.

 Recommendation:
    If your running the appliance/context in transparent mode and your NON-IP packets are
dropped by the appliance, you can configure an ethertype ACL and apply the ACL to an
access group. Note - the appliance ethertype CLI only supports protocol types and not L2
destination MAC     addresses.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: intercept-unexpected
Intercept unexpected packet:
    Either received data from client while waiting for SYNACK from server or received a
packet which cannot be handled in a particular state of TCP intercept.

Recommendation:
```

```
    If this drop is causing the connection to fail, please have a sniffer trace of the
client and server side of the connection while reporting the issue. The box could be under
attack and the sniffer traces or capture would help narrowing down the culprit.
Syslogs:
    None.


----------------------------------------------------------------
Name: no-mcast-entry
FP no mcast entry:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    A multicast entry change has been detected after a packet was punted to the CP, and
the NP can no longer forward the packet since no entry is present.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: no-mcast-intrf
FP no mcast output intrf:
    All output interfaces have been removed from the multicast entry.
    - OR -
    The multicast packet could not be forwarded.

Recommendation:
    Verify that there are no longer any receivers for this group.
    - OR -
    Verify that a flow exists for this packet.

Syslogs:
    None


----------------------------------------------------------------
Name: fragment-reassembly-failed
Fragment reassembly failed:
    This counter is incremented when the appliance fails to reassemble a chain of
fragmented packets into a single packet. All the fragment packets in the chain are
dropped. This is most probably because of failure while allocating memory for the
reassembled packet.

Recommendation:
    Use the show blocks command to monitor the current block memory.

Syslogs:
    None


----------------------------------------------------------------
Name: ifc-classify
Virtual firewall classification failed:
    A packet arrived on a shared interface, but failed to classify to any specific context
interface.

Recommendation:
```

```
    For software versions without customizable mac-address support, use the "global" or
"static" command to specify the IPv4 addresses that belong to each context interface.  For
software versions with customizable mac-address support, enable "mac-address auto" in
system context.  Alternatively, configure unique MAC addresses for each context interfaces
residing over a shared interface with "mac-address" command under each context interface
submode.

Syslogs:
    None.


----------------------------------------------------------------
Name: interface-down
Interface is down:
    This counter will increment for each packet received on an interface that is shutdown
via the 'shutdown' interface sub-mode command. For ingress traffic, the packet is dropped
after security context classification and if the interface associated with the context is
shut down.  For egress traffic, the packet is dropped when the egress interface is shut
down.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-app-length
Invalid App length:
    This counter will increment when the appliance detects an invalid length of the Layer
7 payload in the packet.  Currently, it counts the drops by the DNS Guard function only.
Example: Incomplete DNS header.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-buffer-full
Loopback buffer full:
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface and there is no
buffer space in loopback queue.

Recommendations:
    Check system CPU to make sure it is not overloaded.

Syslogs:
    None


----------------------------------------------------------------
Name: non-ip-pkt-in-routed-mode
Non-IP packet received in routed mode:
    This counter will increment when the appliance receives a packet which is NOT IPv4,
IPv6 or ARP and the appliance/context is configured for ROUTED mode. In normal operation
such packets should be dropped by the default L2 ACL configuration.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.
```

```
 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: host-move-pkt
FP host move packet:
    This counter will increment when the appliance/context is configured for transparent
and source interface of a known L2 MAC address is detected on a different interface.

 Recommendation:
    This indicates that a host has been moved from one interface (i.e. LAN segment) to
another. This condition is normal while in transparent mode if the host has in fact been
moved. However, if the host move toggles back and forth between interfaces, a network loop
may be present.

 Syslogs:
    412001, 412002, 322001


----------------------------------------------------------------
Name: tfw-no-mgmt-ip-config
No management IP address configured for TFW:
    This counter is incremented when the security appliance receives an IP packet in
transparent mode and has no management IP address defined. The packet is dropped.

Recommendation:
    Configure the device with management IP address and mask values.

Syslogs:
    322004


----------------------------------------------------------------
Name: shunned
Packet shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: rm-conn-limit
RM connection limit reached:
    This counter is incremented when the maximum number of connections for a context or
the system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-conn-rate-limit
```

```
RM connection rate limit reached:
    This counter is incremented when the maximum connection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: np-socket-closed
Dropped pending packets in a closed socket:
    If a socket is abruptly closed, by the user or software, then any pending packets in
the pipeline for that socket are also dropped. This counter is incremented for each packet
in the pipeline that is dropped.

Recommendation:
    It is common to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-pf-queue-full
Port Forwarding Queue Is Full:
       This counter is incremented when the Port Forwarding  application's internal queue
is full and it receives another packet  for transmission.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-delete-in-progress
SVC Module received data while connection was being deleted:
    This counter will increment when the security appliance receives a packet associated
with an SVC connection that is in the process of being deleted.

Recommendation:
    This is a normal condition when the SVC connection is torn down for any reason. If
this error occurs repeatedly or in large numbers, it could indicate that clients are
having network connectivity issues.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-bad-framing
SVC Module received badly framed data:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software that it is unable to decode.
```

```
Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-bad-length
SVC Module received bad data length:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software where the calculated and specified lengths do not match.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-unknown-type
SVC Module received unknown data frame:
    This counter will increment when the security appliance receives a packet from an SVC
where the data type is unknown.

Recommendation:
    Validate that the SVC being used by the client is compatible with the version of
security appliance software.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-addr-renew-response
SVC Module received address renew response data frame:
    This counter will increment when the security appliance receives an Address Renew
Response message from an SVC. The SVC should not be sending this message.

Recommendation:
    This indicates that an SVC software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-prepend
SVC Module does not have enough space to insert header:
    This counter will increment when there is not enough space before the packet data to
prepend a MAC header in order to put the packet onto the network.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-channel
```

```
SVC Module does not have a channel for reinjection:
    This counter will increment when the interface that the encrypted data was received
upon cannot be found in order to inject the decrypted data.

Recommendation:
    If an interface is shut down during a connection, this could happen; re-enable/check
the interface. Otherwise, this indicates that a software error should be reported to the
Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-session
SVC Module does not have a session:
    This counter will increment when the security appliance cannot determine the SVC
session that this data should be transmitted over.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-decompres-error
SVC Module decompression error:
    This counter will increment when the security appliance encounters an error during
decompression of data from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-compress-error
SVC Module compression error:
    This counter will increment when the security appliance encounters an error during
compression of data to an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-no-mac
SVC Module unable to find L2 data for frame:
    This counter will increment when the security appliance is unable to find an L2 MAC
header for data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
```

```
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac
SVC Module found invalid L2 data in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
header attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac-len
SVC Module found invalid L2 data length in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
length attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-flow-control
SVC Session is in flow control:
    This counter will increment when the security appliance needs to drop data because an
SVC is temporarily not accepting any more data.

Recommendation:
    This indicates that the client is unable to accept more data. The client should reduce
the amount of traffic it is attempting to receive.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-fragment
SVC Module unable to fragment packet:
    This counter is incremented when a packet to be sent to the SVC is not permitted to be
fragmented or when there are not enough data buffers to fragment the packet.

Recommendation:
    Increase the MTU of the SVC to reduce fragmentation. Avoid using applications that do
not permit fragmentation. Decrease the load on the device to increase available data
buffers.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-dpp-invalid
Invalid packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives a packet from the internal data plane
interface but could not find the proper driver to parse it.
```

```
Recommendation:
    The data plane driver is dynamically registered depending on the type of SSM installed
in the system. So this could happen if data plane packets arrive before the security
appliance is fully initialized. This counter is usually 0. You should not be concerned if
there are a few drops. However, if this counter keeps rising when system is up and
running, it may indicate a problem. Please contact Cisco Technical Assistance Center (TAC)
if you suspect it affects the normal operation of your the security appliance.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-asdp-invalid
Invalid ASDP packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives an ASA SSM Dataplane Protocol (ASDP)
packet from the internal data plane interface, but the driver encountered a problem when
parsing the packet. ASDP is a protocol used by the security appliance to communicate with
certain types of SSMs, like the CSC-SSM. This could happen for various reasons, for
example ASDP protocol version is not compatible between the security appliance and SSM, in
which case the card manager process in the control plane issues system messages and CLI
warnings to inform you of the proper version of images that need to be installed; the ASDP
packet belongs to a connection that has already been terminated on the security appliance;
the security appliance has switched to the standby state (if failover is enable) in which
case it can no longer pass traffic; or any unexpected value when parsing the ASDP header
and payload.

Recommendation:
    The counter is usually 0 or a very small number. But user should not be concerned if
the counter slowly increases over the time, especially when there has been a failover, or
you have manually cleared connections on the security appliance via CLI. If the counter
increases drastically during normal operation, please contact Cisco Technical Assistance
Center (TAC).

Syslogs:
    421003
    421004


----------------------------------------------------------------
Name: ssm-app-request
Service module requested drop:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
drop a packet.

Recommendation:
    More information could be obtained by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with your SSM for
instructions.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-app-fail
Service module is down:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a packet to be inspected by the SSM is dropped because the SSM has become
unavailable. Some examples of this are: software or hardware failure, software or
signature upgrade, or the module being shut down.
```

```
Recommendation:
    The card manager process running in the security appliance control plane would have
issued system messages and CLI warning to inform you of the failure. Please consult the
documentation that comes with the SSM to trouble shoot the SSM failure. Contact Cisco
Technical Assistance Center (TAC) if needed.

Syslog:
    None.


----------------------------------------------------------------
Name: wccp-return-no-route
No route to host for WCCP returned packet:
    This counter is incremented when a packet is returned from the Cache Engine and the
security appliance does not find a route for the original source of the packet.

Recommendation:
    Verify that a route exists for the source ip address of the packet returned from Cache
Engine.

Syslogs:
    None.


----------------------------------------------------------------
Name: wccp-redirect-no-route
No route to Cache Engine:
    This counter is incremented when the security appliance tries to redirect a packet and
does not find a route to the Cache Engine.

Recommendation:
    Verify that a route exists for Cache Engine.

Syslogs:
   None.


----------------------------------------------------------------
Name: telnet-not-permitted
Telnet not permitted on least secure interface:
    This counter is incremented and packet is dropped when the appliance receives a TCP
SYN packet attempting to establish a TELNET session to the appliance and that packet was
received on the least secure interface.

 Recommendation:
    To establish a TELNET session to the appliance via the least secure interface, first
establish an IPSec tunnel to that interface and then connect the TELNET session over that
tunnel.

 Syslogs:
    402117


----------------------------------------------------------------
Name: vpn-handle-error
VPN Handle Error:
    This counter is incremented when the appliances is unable to create a VPN handle
because the VPN handle already exists.

 Recommendation:
```

```
    It is possible to see this counter increment as part of normal operation However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

 Syslogs:
    None.


----------------------------------------------------------------
Name: host-limit
Host limit exceeded:
    This counter is incremented when the licensed host limit is exceeded.

Recommendation:
    None.

Syslogs:
    450001


----------------------------------------------------------------
```

フローのドロップ理由

```
----------------------------------------------------------------
Name: tunnel-torn-down
Tunnel has been torn down:
    This counter will increment when the appliance receives a packet associated with an
established flow whose IPSec security association is in the process of being deleted.

Recommendation:
    This is a normal condition when the IPSec tunnel is torn down for any reason.

Syslogs:
    None


----------------------------------------------------------------
Name: out-of-memory
No memory to complete flow:
    This counter is incremented when the appliance is unable to create a flow because of
insufficient memory.

Recommendation:
    Verify that the box is not under attack by checking the current connections. Also
verify if the configured timeout values are too large resulting in idle flows residing in
memory longer. Check the free memory available by issuing 'show memory'.  If free memory
is low, issue the command 'show processes memory' to determine which processes are
utilizing most of the memory.

Syslogs:
    None


----------------------------------------------------------------
Name: parent-closed
Parent flow is closed:
    When the parent flow of a subordinating flow is closed, the subordinating flow is also
closed.  For example, an FTP data flow (subordinating flow) will be closed with this
specific reason when its control flow (parent flow) is terminated.  This reason is also
given when a secondary flow (pin-hole) is closed by its controlling application.  For
example, when the BYE messaged is received, the SIP inspection engine (controlling
application) will close the corresponding SIP RTP flows (secondary flow).
```

```
Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: closed-by-inspection
Flow closed by inspection:
    This reason is given for closing a flow due to an error detected during application
inspection.  For example, if an error is detected during inspecting an H323 message, the
corresponding H323 flow is closed with this reason.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: fo-primary-closed
Failover primary closed:
    Standby unit received a flow delete message from the active unit and terminated the
flow.

Recommendation:
    If the appliance is running stateful failover, then this counter should increment for
every replicated connection that is torn down on the standby appliance.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo-standby
Flow closed by failover standby:
    If a through-the-box packet arrives at an appliance or context is in a Standby state,
and a flow is created, the packet is dropped and the flow removed.  This counter will
increment each time a flow is removed in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo_rep_err
Standby flow replication error:
    Standby unit failed to replicate a flow.

Recommendation:
    If appliance is processing VPN traffic, then this counter could be constantly
increasing on the standby unit because of the flow could be replicated before the IKE SA
info. No action is required in this case. If the appliance is not processing VPN traffic,
then this indicate a software detect, turn on the debug: "debug fover fail" on the standby
unit, collect the debug output, and report the problem to Cisco TAC.

Syslogs:
```

```
    302014, 302016, 302018


----------------------------------------------------------------
Name: loopback
Flow is a loopback:
    This reason is given for closing a flow due to the following conditions: 1) when
U-turn traffic is present on the flow, and, 2) 'same-security-traffic permit
intra-interface' is not configured.

Recommendation:
    To allow U-turn traffic on an interface, configure the interface with
'same-security-traffic permit intra-interface'.

Syslogs:
    None.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by access rule:
     This counter is incremented when a drop rule is hit by the packet and flow creation
is denied. This rule could be a default rule created when the box comes up, when various
features are turned on or off, when an acl is applied to interface or any other feature
etc. Apart from default rule drops, a flow could be denied because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface
     5) Implicity deny 'ip any any' at the end of an ACL

Recommendation:
    Observe if one of syslogs related to packet drop are fired. Flow drop results in the
corresponding packet-drop that would fire requisite syslog.

Syslogs:
    None.


----------------------------------------------------------------
Name: pinhole-timeout
Pinhole timeout:
    This counter is incremented to report that the appliance opened a secondary flow, but
no packets passed through this flow within the timeout interval, and hence it was removed.
An example of a secondary flow is the FTP data channel that is created after successful
negotiation on the FTP control channel.

Recommendation:
    No action required.

Syslogs:
    302014, 302016


----------------------------------------------------------------
Name: host-removed
Host is removed:
    Flow removed in response to "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002
```

```
-------------------------------------------------------------------
Name: xlate-removed
Xlate Clear:
    Flow removed in response to "clear xlate" or "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


-------------------------------------------------------------------
Name: connection-timeout
Connection timeout:
    This counter is incremented when a flow is closed because of the expiration of it's
inactivity timer.

Recommendation:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021


-------------------------------------------------------------------
Name: conn-limit-exceeded
Connection limit exceeded:
    This reason is given for closing a flow when the connection limit has been exceeded.
The connection limit is configured via the 'set connection conn-max' action command.

Recommendation:
    None.

Syslogs:
    201011


-------------------------------------------------------------------
Name: tcp-fins
TCP FINs:
    This reason is given for closing a TCP flow when TCP FIN packets are received.

Recommendations:
    This counter will increment for each TCP connection that is terminated normally with
FINs.

Syslogs:
    302014


-------------------------------------------------------------------
Name: syn-timeout
SYN Timeout:
    This reason is given for closing a TCP flow due to expiry of embryonic timer.

Recommendations:
    If these are valid session which take longer to establish a connection increase the
embryonic timeout.

Syslogs:
    302014
```

```
----------------------------------------------------------------
Name: fin-timeout
FIN Timeout:
    This reason is given for closing a TCP flow due to expiry of half-closed timer.

Recommendations:
    If these are valid session which take longer to close a TCP flow, increase the
half-closed timeout.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-in
TCP Reset-I:
    This reason is given for closing an outbound flow (from a low-security interface to a
same- or high-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-out
TCP Reset-O:
    This reason is given for closing an inbound flow (from a high-security interface to
low-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-appliance
TCP Reset-APPLIANCE:
    This reason is given for closing a flow when a TCP reset is generated by appliance.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: recurse
Close recursive flow:
    A flow was recursively freed.  This reason applies to pair flows and multicast slave
flows, and serves to prevent syslogs being issued for each of these subordinate flows.

Recommendation:
    No action required.

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-intecept-no-response
TCP intercept, no response from server:
    SYN retransmission timeout after trying three times, once every second. Server
unreachable, tearing down connection.

Recommendation:
    Check if the server is reachable from the ASA.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-unexpected
TCP intercept unexpected state:
    Logic error in TCP intercept module, this should never happen.

Recommendation:
    Indicates memory corruption or some other logic error in the TCP intercept module.

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This reason is given for closing a TCP flow when check-retranmission feature is
enabled and the TCP endpoint sent a retranmission with different data from the original
packet.

Recommendations:
    The TCP endpoint maybe attacking by sending different data in TCP retransmits. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This reason is given for closing a TCP flow when window size advertized by TCP
endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow this connection, use the window-variation configuration under
tcp-map.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-invalid-syn
TCP invalid SYN:
    This reason is given for closing a TCP flow when the SYN packet is invalid.

Recommendations:
```

```
    SYN packet could be invalid for number of reasons, like invalid checksum, invalid TCP
header. Please use the packet capture feature to understand why the SYN packet is invalid.
If you would like to allow these connection use tcp-map configurations to bypass checks.

Syslogs:
    302014


----------------------------------------------------------------
Name: mcast-intrf-removed
Multicast interface removed:
    An output interface has been removed from the multicast entry.
    - OR -
    All output interfaces have been removed from the multicast entry.

Recommendation:
    No action required.
    - OR -
    Verify that there are no longer any receivers for this group.

Syslogs:
    None


----------------------------------------------------------------
Name: mcast-entry-removed
Multicast entry removed:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    The multicast entry has been deleted so the flow is being cleaned up, but the packet
will be reinjected into the data path.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-kill
Flow terminated by TCP Intercept:
    TCP intercept would teardown a connection if this is the first SYN, a connection is
created for the SYN, and TCP intercept replied with a SYN cookie, or after seeing a valid
ACK from client, when TCP intercept sends a SYN to server, server replies with a RST.

Recommendation:
    TCP intercept normally does not create a connection for first SYN, except when there
are nailed rules or the packet comes over a VPN tunnel or the next hop gateway address to
reach the client is not resolved. So for the first SYN this indicates that a connection
got created. When TCP intercept receives a RST from server, its likely the corresponding
port is closed on the server.

Syslogs:
    None


----------------------------------------------------------------
Name: audit-failure
Audit failure:
```

```
    A flow was freed after matching an "ip audit" signature that had reset as the
associated action.

Recommendation:
    If removing the flow is not the desired outcome of matching this signature, then
remove the reset action from the "ip audit" command.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-request
Flow terminated by IPS:
    This reason is given for terminating a flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: ips-fail-close
IPS fail-close:
    This reason is given for terminating a flow since IPS card is down and fail-close
option was used with IPS inspection.

Recommendations:
    Check and bring up IPS card

Syslogs:
    420001


----------------------------------------------------------------
Name: reinject-punt
Flow terminated by punt action:
    This counter is incremented when a packet is punted to the exception-path for
processing by one of the enhanced services such as inspect, aaa etc and the servicing
routine, having detected a violation in the traffic flowing on the flow, requests that the
flow be dropped. The flow is immediately dropped.

Recommendation:
    Please watch for syslogs fired by servicing routine for more information. Flow drop
terminates the corresponding connection.

Syslogs:
    None.


----------------------------------------------------------------
Name: shunned
Flow shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.  When a shun command is applied, it will be
incremented for each existing flow that matches the shun command.

Recommendation:
    No action required.

Syslogs:
    401004
```

```
-------------------------------------------------------------
Name: host-limit
host-limit

-------------------------------------------------------------
Name: nat-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".  Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.  For dynamic NAT, ensure
that each "nat" command is paired with at least one "global" command.  Use "show nat" and
"debug pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


-------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host. Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005


-------------------------------------------------------------
Name: no-ipv6-ipsec
IPSec over IPv6 unsupported:
    This counter will increment when the appliance receives an IPSec ESP packet, IPSec
NAT-T ESP packet or an IPSec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPSec sessions encapsulated in IP version 6.

Recommendation:
    None

Syslogs:
    None


-------------------------------------------------------------
Name: tunnel-pending
Tunnel being brought up or torn down:
    This counter will increment when the appliance receives a packet matching an entry in
the security policy database (i.e. crypto map) but the security association is in the
process of being negotiated; its not complete yet.

    This counter will also increment when the appliance receives a packet matching an
entry in the security policy database but the security association has been or is in the
process of being deleted. The difference between this indication and the 'Tunnel has been
torn down' indication is that the 'Tunnel has been torn down' indication is for
established flows.

Recommendation:
```

```
    This is a normal condition when the IPSec tunnel is in the process of being negotiated
or deleted.

Syslogs:
    None


------------------------------------------------------------------
Name: need-ike
Need to start IKE negotiation:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPSec security association. This is generally a normal
condition for LAN-to-LAN IPSec configurations. This indication will cause the appliance to
begin ISAKMP negotiations  with the destination peer.

Recommendation:
    If you have configured IPSec LAN-to-LAN on your appliance, this indication is normal
and does not indicate a problem.  However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing.

    Verify that you can communicate with the destination peer and verify your crypto
configuration via the 'show running-config' command.

Syslogs:
    None


------------------------------------------------------------------
Name: vpn-handle-error
VPN handle error:
    This counter is incremented when the appliance is unable to create a VPN handle
because the VPN handle already exists.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-error
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


------------------------------------------------------------------
Name: vpn-handle-not-found
VPN handle not found:
    This counter is incremented when a datagram hits an encrypt or decrypt rule, and no
VPN handle is found for the flow the datagram is on.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-not-found
    show asp table classify crypto
```

```
    show asp table vpn-context detail

Syslogs:
    None


------------------------------------------------------------------
Name: inspect-fail
Inspection failure:
    This counter will increment when the appliance fails to enable protocol inspection
carried out by the NP for the connection. The cause could be memory allocation failure, or
for ICMP error message, the appliance not being able to find any established connection
related to the frame embedded in the ICMP error message.

Recommendation:
    Check system memory usage.  For ICMP error message, if the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004 for ICMP error.


------------------------------------------------------------------
Name: no-inspect
Failed to allocate inspection:
    This counter will increment when the security appliance fails to allocate a run-time
inspection data structure upon connection creation. The connection will be dropped.

Recommendation:
    This error condition is caused when the security appliance runs out of system memory.
Please check the current available free memory by executing the "show memory" command.

Syslogs:
    None


------------------------------------------------------------------
Name: reset-by-ips
Flow reset by IPS:
    This reason is given for terminating a TCP flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420003


------------------------------------------------------------------
Name: flow-reclaimed
Non-tcp/udp flow reclaimed for new request:
    This counter is incremented when a reclaimable flow is removed to make room for a new
flow.  This occurs only when the number of flows through the appliance equals the maximum
number permitted by the software imposed limit, and a new flow request is received. When
this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels
permitted by the appliance, then the oldest reclaimable flow is removed to make room for
the new flow.  All flows except the following are deemed to be reclaimable:
    1. TCP, UDP, GRE and Failover flows
    2. ICMP flows if ICMP stateful inspection is enabled
    3. ESP flows to the appliance

Recommendation:
```

```
    No action is required if this counter is incrementing slowly. If this counter is
incrementing rapidly, it could mean that the appliance is under attack and the appliance
is spending more time reclaiming and rebuilding flows.

Syslogs
    302021


----------------------------------------------------------------
Name: non_tcp_syn
non-syn TCP:
    This reason is given for terminating a TCP flow when the first packet is not a SYN
packet.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof-detect
IPSec spoof packet detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.  The packet matched the inner header security policy check of
a configured and established IPSec connection on the appliance but was received
unencrypted.  This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

Syslogs:
    402117


----------------------------------------------------------------
Name: rm-xlate-limit
RM xlate limit reached:
    This counter is incremented when the maximum number of xlates for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-host-limit
RM host limit reached:
    This counter is incremented when the maximum number of hosts for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001
```

```
----------------------------------------------------------------
Name: rm-inspect-rate-limit
RM inspect rate limit reached:
    This counter is incremented when the maximum inspection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: tcpmod-connect-clash
A TCP connect socket clashes with an existing listen connection.  This is an internal
system error.  Contact TAC.

----------------------------------------------------------------
Name: svc-spoof-detect
SVC spoof packet detected:
    This counter will increment when the security appliance receives a packet which should
have been encrypted but was not. The packet matched the inner header security policy check
of a configured and established SVC connection on the security appliance but was received
unencrypted. This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed SVC traffic.

Syslogs:
    None


----------------------------------------------------------------
Name: ssm-app-request
Flow terminated by service module:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
terminate a connection.

Recommendation:
    You can obtain more information by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with comes with
the SSM for instructions.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-app-fail
Service module failed:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a connection that is being inspected by the SSM is terminated because the
SSM has failed.

Recommendation:
```

The card manager process running in the security appliance control plane issued system messages and CLI warning to inform you of the failure. Please consult the documentation that comes with the SSM to trouble shoot the SSM failure. Contact Cisco Technical Assistance Center (TAC) if needed.

Syslog:
421001.

Name: ssm-app-incompetent
Service module incompetent:
This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a connection is supposed to be inspected by the SSM, but the SSM is not able to inspect it. This counter is reserved for future use. It should always be 0 in the current release.

Recommendation:
None.

Syslog:
None.

Name: ssl-bad-record-detect
SSL bad record detected:
This counter is incremented for each unknown SSL record type received from the remote peer. Any unknown record type received from the peer is treated as a fatal error and the SSL connections that encounter this error must be terminated.

Recommendation:
It is not normal to see this counter increment at any time. If this counter is incremented, it usually means that the SSL protocol state is out of sync with the client software. The most likely cause of this problem is a software defect in the client software. Contact the Cisco TAC with the client software or web browser version and provide a network trace of the SSL data exchange to troubleshoot this problem.

Syslogs:
None.

Name: ssl-handshake-failed
SSL handshake failed:
This counter is incremented when the TCP connection is dropped because the SSL handshake failed.

Recommendation:
This is to indicate that the TCP connection is dropped because the SSL handshake failed. If the problem cannot be resolved based on the syslog information generated by the handshake failure condition, please include the related syslog information when contacting the Cisco TAC.

Syslogs:
725006.
725014.

Name: ssl-malloc-error
SSL malloc error:

```
    This counter is incremented for each malloc failure that occurs in the SSL lib.  This
is to indicate that SSL encountered a low memory condition where it can't allocate a
memory buffer or packet block.

Recommendation:
    Check the security appliance memory and packet block condition and contact Cisco the
TAC with this memory information.

Syslogs:
    None.


----------------------------------------------------------------
Name: ctm-crypto-request-error
CTM crypto request error:
    This counter is incremented each time CTM cannot accept our crypto request.  This
usually means the crypto hardware request queue is full.

Recommendation:
    Issue the show crypto protocol statistics ssl command and contact the Cisco TAC with
this information.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssl-record-decrypt-error
SSL record decryption failed:
    This counter is incremented when a decryption error occurs during SSL data receive.
This usually means that there is a bug in the SSL code of the ASA or peer, or an attacker
may be modifying the data stream. The SSL connection has been closed.

Recommendation:
    Investigate the SSL data streams to and from your ASA. If there is no attacker, then
this indicates a software error that should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: np-socket-conn-not-accepted
A new socket connection was not accepted:
    This counter is incremented for each new socket connection that is not accepted by the
security appliance.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-failure
NP socket failure:
    This is a general counter for critical socket processing errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.
```

```
Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-data-move-failure
NP socket data movement failure:
    This counter is incremented for socket data movement errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-new-conn-failure
NP socket new connection failure:
    This counter is incremented for new socket connection failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-transport-closed
NP socket transport closed:
    This counter is incremented when the transport attached to the socket is abruptly
closed.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-block-conv-failure
NP socket block conversion failure:
    This counter is incremented for socket block conversion failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: ssl-received-close-alert
SSL received close alert:
    This counter is incremented each time the security appliance receives a close alert
from the remote client.  This indicates that the client has notified us they are going to
drop the connection.  It is part of the normal disconnect process.
```

```
Recommendation:
    None.

Syslog:
    725007.


------------------------------------------------------------------
Name: svc-failover
An SVC socket connection is being disconnected on the standby unit:
    This counter is incremented for each new SVC socket connection that is disconnected
when the active unit is transitioning into standby state as part of a failover transition.

Recommendation:
    None. This is part of a normal cleanup of a SVC connection when the current device is
transitioning from active to standby. Existing SVC connections on the device are no longer
valid and need to be removed.

Syslogs:
    None.


------------------------------------------------------------------
Name: children-limit
Max per-flow children limit exceeded:
    The number of children flows associated with one parent flow exceeds the internal
limit of 200.

Recommendation:
    This message indicates either a misbehaving application or an active attempt to
exhaust the firewall memory.  Use "set connection per-client-max" command to further fine
tune the limit.  For FTP, additionally enable the "strict" option in "inspect ftp".

Syslogs:
    210005


------------------------------------------------------------------
Name: tracer-flow
packet-tracer traced flow drop:
    This counter is internally used by packet-tracer for flow freed once tracing is
complete.

Recommendation:
    None.

Syslog:
    None.


------------------------------------------------------------------
Name: sp-looping-address
looping-address:
    This counter is incremented when the source and destination addresses in a flow are
the same.  SIP flows where address privacy is enabled are excluded, as it is normal for
those flows to have the same source and destination address.

 Recommendation:
    There are two possible conditions when this counter will increment. One is when the
appliance receives a packet with the source address equal to the destination. This
represents a type of DoS attack.  The second is when the NAT configuration of the
appliance NATs a source address to equal that of the destination.  One should examine
```

```
syslog message 106017 to determine what IP address is causing the counter to increment,
then enable packet captures to capture the offending packet, and perform additional
analysis.

 Syslogs:
    106017


----------------------------------------------------------------
Name: vpn-context-expired
Expired VPN context:
    This counter will increment when the security appliance receives a packet that
requires encryption or decryption, and the ASP VPN context required to perform the
operation is no longer valid.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    None


----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter will increment when the security appliance receives a packet on an
existing flow that no longer has a valid output adjacency. This can occur if the nexthop
is no longer reachable or if a routing change has occurred typically in a dynamic routing
environment.

 Recommendation:
    No action required.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-selector-failure
IPSec VPN inner policy selector mismatch detected:
    This counter is incremented when an IPSec packet is received with an inner IP header
that does not match the configured policy for the tunnel.

 Recommendation:
    Verify that the crypto ACLs for the tunnel are correct and that all acceptable packets
are included in the tunnel identity.  Verify that the box is not under attack if this
message is repeatedly seen.

 Syslogs:
    402116


----------------------------------------------------------------
Name: np-midpath-service-failure
NP midpath service failure:
    This is a general counter for critical midpath service errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.
```

```
----------------------------------------------------------------
Name: svc-replacement-conn
SVC replacement connection established:
    This counter is incremented when an SVC connection is replaced by a new connection.

Recommendation:
    None. This may indicate that users are having difficulty maintaining connections to
the ASA. Users should evaluate the quality of their home network and Internet connection.

Syslog:
    722032


----------------------------------------------------------------
```

例

次に、**show asp drop** コマンドの出力例を示します。タイムスタンプが、カウンタが最後にクリアされた時間を示しています。

```
hostname# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                          3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                      4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                         760
  Expired flow (flow-expired)                                           1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                             24
  NAT failed (nat-failed)                                           28739
  NAT reverse path failed (nat-rpf-failed)                          22266
  Inspection failure (inspect-fail)                                 19433

Last clearing: 17:02:12 UTC Jan 17 2008 by enable_15
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp drop コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	高速セキュリティ パスのドロップ統計情報をクリアします。
show conn	接続に関する情報を表示します。

show asp table arp

高速セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

構文の説明

address *ip_address*	（任意）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（任意）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（任意）IP アドレスのサブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show arp コマンドがコントロール プレーンの内容を表示するのに対して、**show asp table arp** コマンドは高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

高速セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類ルールと対応付けます。それぞれのルールには、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。

show asp table classify [**hit** | **crypto** | **domain** *domain_name* | **interface** *interface_name*]

構文の説明

domain *domain_name*	（任意）特定の分類子ドメインのエントリを表示します。ドメインのリストについては、「使用上のガイドライン」を参照してください。
hits	（任意）0 以外のヒット値を持つ分類子エントリを表示します。
interface *interface_name*	（任意）分類子テーブルを表示する特定のインターフェイスを指定します。
crypto	（任意）暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)	**hits** オプション、および asp テーブルのカウンタが最後にクリアされたのがいつかを示すタイムスタンプが追加されました。
8.0(2)	tmatch コンパイルが中止された回数を示すために、新しいカウンタが追加されました。このカウンタは、値が 0 より大きい場合のみ表示されます。

使用上のガイドライン

show asp table classifier コマンドは、高速セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

分類子ドメインには、次のものがあります。

```
aaa-acct
aaa-auth
aaa-user
```

```
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
priority-q
punt
```

```
punt-l2
punt-root
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

次に、**show asp table classify hits** コマンドの出力例を示します。ヒット カウンタの最後のクリアのレコードが示されています。

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp table interfaces

高速セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table interfaces コマンドは、高速セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
```

```
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show asp table routing

高速セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

構文の説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ（/）に続けてプレフィックス（0 ～ 128）を入力し、サブネット マスクを含めることができます。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（任意）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合は、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table routing コマンドは、高速セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
```

```
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

関連コマンド

コマンド	説明
show route	コントロール プレーン内のルーティング テーブルを表示します。

show asp table socket

アクセラレーション セキュリティ パスのソケット情報をデバッグするには、特権 EXEC モードで **show asp table socket** コマンドを使用します。

show asp table socket

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table socket コマンドを実行すると、アクセラレーション セキュリティ パスのソケット情報をデバッグできます。

例

次に、**show asp table socket** コマンドの例を示します。

```
Protocol  Socket    Local Address              Foreign Address         State
TCP       00012bac  10.86.194.224:23           0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22           0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443            0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22           171.69.137.139:4190     ESTAB
```

関連コマンド

コマンド	説明
show asp table vpn-context	アクセラレーション セキュリティ パスの VPN コンテキスト テーブルをデバッグします。

show asp table vpn-context

高速セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

構文の説明

detail	（任意）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(4)	トンネルのドロップ後にステートフル フローを保持する各コンテキストに +PRESERVE フラグが追加されました。

使用上のガイドライン

show asp table vpn-context コマンドは、高速セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context** コマンドの出力例を示します。

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** [**detail**]]

構文の説明

address *hex*	（任意）このアドレスに対応するブロックを 16 進数形式で表示します。
all	（任意）すべてのブロックを表示します。
assigned	（任意）割り当て済みでアプリケーションによって使用されているブロックを表示します。
detail	（任意）一意のキュー タイプごとに最初のブロックの一部（128 バイト）を表示します。
dump	（任意）ヘッダーとパケットの情報を含め、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（任意）ブロックの診断を表示します。
free	（任意）使用可能なブロックを表示します。
header	（任意）ブロックのヘッダーを表示します。
old	（任意）1 分よりも前に割り当てられたブロックを表示します。
packet	（任意）ブロックのヘッダーおよびパケットの内容を表示します。
pool *size*	（任意）特定のサイズのブロックを表示します。
queue history	（任意）セキュリティ アプライアンスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。
summary	（任意）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。
8.0(2)	dupb ブロックは、4 バイト ブロックではなく長さが 0 のブロックを使用するようになりました。0 バイト ブロック用の 1 行が追加されました。

使用上のガイドライン

show blocks コマンドは、セキュリティ アプライアンスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックがセキュリティ アプライアンス経由で伝送されている限り、メモリがいっぱいになっている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが伝送されているかどうかを確認できます。トラフィックが伝送されておらず、かつメモリがいっぱいになっている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の高基準値に関する、システム全体の情報およびコンテキスト固有の情報が含まれます。

出力表示の詳細については、「例」を参照してください。

例

次に、シングル モードでの **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

表 25-1 に、各フィールドの説明を示します。

表 25-1　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。次に例を示します。
0	dupb ブロックで使用されます。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。またこのサイズのブロックは、通常、パケットをドライバに送信するコードなどで使用されます。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。

表 25-1　show blocks のフィールド （続き）

フィールド	説明
256	ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブなセキュリティ アプライアンスは、パケットを生成してスタンバイセキュリティ アプライアンスに送信し、変換と接続のテーブルを更新します。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイセキュリティ アプライアンスに対して更新されなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、セキュリティ アプライアンスの処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態をセキュリティ アプライアンスが維持できない問題が発生します。 セキュリティ アプライアンスから送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバに記録していないことを確認してください。この情報は、セキュリティ アプライアンス コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することを推奨します。
1550	セキュリティ アプライアンスで処理するイーサネット パケットを格納するために使用されます。 パケットは、セキュリティ アプライアンス インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。セキュリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを発信インターフェイス上の出力キューに配置します。セキュリティ アプライアンスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT カラムに示されます）。CNT カラムが 0 になると、セキュリティ アプライアンスはさらにブロックを確保しようとします（最大で 8192 個まで）。使用可能なブロックがなくなった場合、セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御の更新に使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、ブロックの最大数は変化しません。例外は 256 バイト ブロックと 1550 バイト ブロックで、セキュリティ アプライアンスはこれらのブロックを必要に応じてダイナミックに作成できます（最大で 8192 個）。
LOW	低基準値。この数は、セキュリティ アプライアンスの電源がオンになった時点、またはブロックが（**clear blocks** コマンドで）最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。
CNT	特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 25-2 に、各フィールドの説明を示します。

表 25-2　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。alloc、get、put、free の 4 つのいずれかです。
location	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
```

```
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
hostname# show blocks pool 1550 summary
```

```
Class 3, size 1550

=================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

=================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
=================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

=================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

表 25-3 に、各フィールドの説明を示します。

表 25-3　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリでレポートされなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されて内容が無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられるメモリを増やします。

コマンド	説明
clear blocks	システム バッファの統計情報をクリアします。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権 EXEC モードで **show boot** コマンドを使用します。

show bootvar

構文の説明

show bootvar	システムのブート プロパティ。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定します。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ **boot system** コマンドと **boot config** コマンドで設定します。

例

次に、BOOT 変数が disk0:/f1_image を保持している例を示します。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:/f1_backupimage です。これは、BOOT 変数が boot system コマンドで変更されているものの、実行コンフィギュレーションがまだ **write memory** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:/f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブートローダは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:1/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションを指します。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、**boot config** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、**boot config** コマンドで変更して、**write memory** コマンドで保存できます。

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show capture

オプションを何も指定しない場合にキャプチャのコンフィギュレーションを表示するには、**show capture** コマンドを使用します。

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

構文の説明

capture_name	（任意）パケット キャプチャの名前。
access-list *access_list_name*	（任意）特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
count *number*	（任意）指定されたデータのパケット数を表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する isakmp データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。
detail	（任意）各パケットについて、プロトコル情報を追加表示します。
dump	（任意）データ リンク トランスポート経由で転送されたパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC 情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。表 25-4 で角カッコに囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 25-4　パケット キャプチャの出力形式

パケット タイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

例

次に、キャプチャのコンフィギュレーションを表示する例を示します。

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次に、ARP キャプチャによってキャプチャされたパケットを表示する例を示します。

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show chardrop** コマンドの出力例を示します。

```
hostname# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

show checkheaps

checkheaps に関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

show checkheaps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show checkheaps** コマンドの出力例を示します。

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	checkheap の確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 4 つのグループの 16 進数を表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（セキュリティ アプライアンス のフラッシュ パーティションからの読み込み、または フラッシュ パーティションへの書き込み時）。「.」は、セキュリティ アプライアンスが処理に占有されているが「ハングアップ」していないことを示しています。このメッセージは、「system processing, please wait」メッセージと同様です。

例

次に、コンフィギュレーションまたはチェックサムを表示する例を示します。

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、チャンクに関する統計情報を表示する例を示します。

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスを表示するには、名前として **default** と入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show class default** コマンドの出力例を示します。

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。

show clock

セキュリティ アプライアンスに時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

構文の説明

detail	（任意）クロック ソース（NTP またはユーザ コンフィギュレーション）と現在の夏時間設定（存在する場合）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show clock** コマンドの出力例を示します。

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

次に、**show clock detail** コマンドの出力例を示します。

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show compression svc

セキュリティ アプライアンスで SVC 接続の圧縮統計情報を表示するには、特権 EXEC モードで **show compression svc** コマンドを使用します。

show compression svc

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show compression svc** コマンドの出力例を示します。

```
hostname# show compression svc
Compression SVC Sessions                          1
Compressed Frames                            249756
Compressed Data In (bytes)                  0048042
Compressed Data Out (bytes)                 4859704
Expanded Frames                                   1
Compression Errors                                0
Compression Resets                                0
Compression Output Buf Too Small                  0
Compression Ratio                              2.06
Decompressed Frames                          876687
Decompressed Data In                      279300233
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して SVC 接続を介する HTTP データの圧縮をイネーブルにします。

show configuration

セキュリティ アプライアンスでフラッシュ メモリに保存されているコンフィギュレーションを表示するには、特権 EXEC モードで **show configuration** コマンドを使用します。

show configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドが変更されました。

使用上のガイドライン

show configuration コマンドは、セキュリティ アプライアンスのフラッシュ メモリに保存されているコンフィギュレーションを表示します。**show running-config** コマンドとは異なり、**show configuration** コマンドの実行ではそれほど多くの CPU リソースが使用されません。

セキュリティ アプライアンスのメモリ内のアクティブなコンフィギュレーション（保存されているコンフィギュレーションの変更など）を表示するには、**show running-config** コマンドを使用します。

例

次の例では、セキュリティ アプライアンスのフラッシュ メモリに保存されている設定を表示する方法を示します。

```
hostname# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
```

```
 security-level 50
 ip address 40.0.0.5 255.0.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 40.0.0.0 255.0.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
```

```
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

関連コマンド

コマンド	説明
configure	ターミナルからセキュリティ アプライアンスを設定します。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}]
[**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]]
[**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]]

構文の説明

address	（任意）指定した送信元 IP アドレスまたは宛先 IP アドレスとの接続を表示します。
all	（任意）通過トラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（任意）アクティブな接続の数を表示します。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
detail	（任意）変換タイプとインターフェイスの情報を含め、接続の詳細を表示します。
long	（任意）接続をロング フォーマットで表示します。
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定した送信元ポートまたは宛先ポートとの接続を表示します。
protocol {tcp | udp}	（任意）接続プロトコル **tcp** または **udp** を指定します。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
state *state_type*	（任意）接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 25-5 を参照してください。

デフォルト

デフォルトでは、すべての通過接続が表示されます。デバイスへの管理接続も表示するには、**all** キーワードを使用する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	構文が簡略化され、「ローカル」と「外部」の概念の代わりに送信元と宛先の概念を使用するようになりました。新しい構文では、送信元アドレスを最初のアドレスとして入力し、宛先アドレスを 2 番めのアドレスとして入力します。以前の構文では、**foreign** や **fport** などのキーワードを使用して宛先アドレスおよびポートを設定していました。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続および UDP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注） セキュリティ アプライアンスで第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

表 25-5 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。

表 25-5　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続

表 25-5　接続状態のタイプ （続き）

キーワード	表示される接続タイプ
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ インスペクション エンジン接続
vpn_orphan	孤立した VPN トンネル フロー

detail オプションを使用すると、表 25-6 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

表 25-6　接続フラグ

フラグ	説明
a	SYN に対する外部 ACK を待機
A	SYN に対する内部 ACK を待機
B	外部からの初期 SYN
C	Computer Telephony Interface Quick Buffer Encoding（CTIQBE; コンピュータ テレフォニー インターフェイス クイック バッファ エンコーディング）メディア接続。
d	dump
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN
g	メディア ゲートウェイ コントロール プロトコル（MGCP）接続
G	接続がグループの一部。G フラグは、接続がグループの一部であることを示します。GRE および FTP の Strict フィックスアップによって設定され、制御接続と関連するすべてのセカンダリ接続を指定します。制御接続が切断されると、関連するすべてのセカンダリ接続も切断されます。
h	H.225
H	H.323
i	不完全な TCP 接続または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製（未使用）
P	内部バック接続
q	SQL*Net データ

表 25-6　接続フラグ （続き）

フラグ	説明
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC.show conn コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続。UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
T	SIP 接続。UDP 接続の場合、値 T は、timeout sip コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。
U	up
V	VPN の孤立
W	WAAS
X	CSC SSM などのサービス モジュールによって検査

（注）　DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが *DNS サーバの IP アドレス*に置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注）　**timeout conn** コマンドで定義した非アクティブ期間（デフォルトは 1:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

LAN-to-LAN トンネルまたはネットワーク拡張モード トンネルがドロップし、回復しない場合は、孤立したトンネル フローが数多く発生します。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。**show conn** コマンドの出力では、このような孤立したフローを **V** フラグで示します。

例

複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。次に、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示する例を示します。

```
hostname# show conn state up,rpc,h323,sip
```

次に、**show conn count** コマンドの出力例を示します。

```
hostname# show conn count
54 in use, 123 most used
```

次に、**show conn** コマンドの出力例を示します。次に、内部ホスト 10.1.1.15 から 10.10.49.10 の外部 Telnet サーバへの TCP セッション接続の例を示します。B フラグが存在しないため、接続は内部から開始されています。「U」、「I」および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示します。

```
hostname# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

次に、**show conn** コマンドの出力例を示します。接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
hostname# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

次に、**show conn detail** コマンドの出力例を示します。次に、外部ホスト 10.10.49.10 から内部ホスト 10.1.1.15 への UDP 接続の例を示します。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
hostname# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
```

```
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

次に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

関連コマンド

コマンド	説明
clear conn	接続をクリアします。
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
inspect mgcp	MGCP アプリケーション インスペクションをイネーブルにします。
inspect sip	Java アプレットを HTTP トラフィックから削除します。
inspect skinny	SCCP アプリケーション インスペクションをイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例は、コンソール出力がない場合に表示されるメッセージを示しています。

```
hostname# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | **detail** | **count**]

構文の説明

count	（任意）設定済みコンテキストの数を表示します。
detail	（任意）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（任意）コンテキスト名を設定します。名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	割り当てられた IPS 仮想センサーについての情報が追加されました。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show context** コマンドの出力例を示します。この例では、3 つのコンテキストが表示されています。

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 25-7 に、各フィールドの説明を示します。

表 25-7　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	このコンテキストに割り当てられたインターフェイス。
URL	セキュリティ アプライアンスがコンテキストのコンフィギュレーションをロードする URL。

次に、システム実行スペースでの **show context detail** コマンドの出力例を示します。

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 25-8 に、各フィールドの説明を示します。

表 25-8　コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
状態メッセージ：	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。
Has been created, but initial ACL rules not complete	セキュリティ アプライアンスはコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、下位セキュリティ レベルから上位セキュリティ レベルへのトラフィック送信を禁止したり、アプリケーション インスペクションおよびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックがセキュリティ アプライアンスをいっさい通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだセキュリティ アプライアンスがコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、ブランクの実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。

表 25-8　コンテキストの状態 （続き）

フィールド	説明
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Real Interfaces	このコンテキストに割り当てられたインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはインターフェイスの実際の名前です。
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Real IPS Sensors	AIP SSM をインストールしている場合に、コンテキストに割り当てられる IPS 仮想センサー。センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはセンサーの実際の名前です。
Mapped IPS Sensors	センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。センサー名をマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

次に、**show context count** コマンドの出力例を示します。

```
hostname# show context count
Total active contexts: 2
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

show controller

存在するすべてのインターフェイスについて、コントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [*physical_interface*] [**detail**]

構文の説明

detail	（任意）コントローラの詳細を表示します。
physical_interface	（任意）インターフェイス ID を指定します。

デフォルト

スイッチ ポートを指定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	このコマンドは ASA 5505 のみではなく、すべてのプラットフォームに適用されるようになりました。**detail** キーワードが追加されました。

使用上のガイドライン

このコマンドは、内部的不具合やカスタマーにより発見された不具合を調査するときに、Cisco TAC がコントローラについての有用なデバッグ情報を収集するために役立ちます。実際の出力は、モデルとイーサネット コントローラによって異なります。

例

次に、**show controller** コマンドの出力例を示します。

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
```

```
          Port Ctrl-1:   0x0000  Vlan Map:      0x077f
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0080
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

      Global Registers:
          Control:       0x0482

-------------------------------------------------------------------
Number of VLANs: 1
-------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
-------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-------------------------------------------------------------------

Ethernet0/1:
   Marvell 88E6095 revision 2, switch port 6
     PHY Register:
          Control:       0x3000  Status:        0x7849
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x0000
          Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x0130
          PHY Status:    0x0040  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0007  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07bf
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0040
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/2:
   Marvell 88E6095 revision 2, switch port 5
     PHY Register:
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07df
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0020
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/3:
   Marvell 88E6095 revision 2, switch port 4
     PHY Register:
          Control:       0x3000  Status:        0x786d
```

```
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07ef
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0010
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/4:
   Marvell 88E6095 revision 2, switch port 3
     PHY Register:
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07f7
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0008
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/5:
   Marvell 88E6095 revision 2, switch port 2
     PHY Register:
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07fb
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0004
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
          Control:       0x3000  Status:        0x7849
          Identifier1:   0x0141  Identifier2:   0x0c85
```

```
        Auto Neg:      0x01e1  LP Ability:    0x0000
        Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
        PHY Status:    0x0040  PHY Intr En:   0x8400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
        Status:        0x0007  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0002
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
    ----Inline power related counters and registers----
    Power on fault: 0  Power off fault: 0
    Detect enable fault: 0  Detect disable fault: 0
    Faults: 0
    Driver counters:
    I2C Read Fail: 0   I2C Write Fail: 0
    Resets: 1  Initialized: 1
    PHY reset error: 0
    LTC4259 registers:
    INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
    DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
    SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
    PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
    OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
    TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Ethernet0/7:
    Marvell 88E6095 revision 2, switch port 0
      PHY Register:
        Control:       0x3000  Status:        0x7849
        Identifier1:   0x0141  Identifier2:   0x0c85
        Auto Neg:      0x01e1  LP Ability:    0x0000
        Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
        PHY Status:    0x0040  PHY Intr En:   0x8400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
        Status:        0x0007  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07fe
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0001
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
    ----Inline power related counters and registers----
    Power on fault: 0  Power off fault: 0
    Detect enable fault: 0  Detect disable fault: 0
    Faults: 0
    Driver counters:
    I2C Read Fail: 0   I2C Write Fail: 0
    Resets: 1  Initialized: 1
    PHY reset error: 0
    LTC4259 registers:
    INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
    DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
    SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
    PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
```

```
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                          0xe0004000 = 0x00000000
    ctrl_status                  0xe0004004 = 0x5501064a
    irq_src                      0xe0004008 = 0x00000000
    irq_msk                      0xe000400c = 0x00000000
    irq_hw_err_src               0xe0004010 = 0x00000000
    irq_hw_err_msk               0xe0004014 = 0x00001000
    bmu_cs_rxq                   0xe0004060 = 0x002aaa80
    bmu_cs_stxq                  0xe0004068 = 0x01155540
    bmu_cs_atxq                  0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:
    mac_addr1_lo                 0xe0004100 = 0x00000000
    mac_addr1_hi                 0xe0004104 = 0x00000000
    mac_addr2_lo                 0xe0004108 = 0x00000000
    mac_addr2_hi                 0xe000410c = 0x00000000
    mac_addr3_lo                 0xe0004110 = 0x00000000
    mac_addr3_hi                 0xe0004114 = 0x00000000
    chip_info                    0xe0004118 = 0xb0110000
    eprom                        0xe000411c = 0x00000000
    flash_addr_reg               0xe0004120 = 0x0001fffe
    flash_data_port              0xe0004124 = 0x000000ff
    loader                       0xe0004128 = 0x00000400
    timer_init_val               0xe0004130 = 0x00000000
    timer_val                    0xe0004134 = 0x00000000
    timer_ctrl                   0xe0004138 = 0x00000202
    irq_mod_timer_init_val       0xe0004140 = 0x00000000
    irq_mod_timer                0xe0004144 = 0x00000000
    irq_mod_timer_ctrl           0xe0004148 = 0x00000202
    irq_mod_msk                  0xe000414c = 0x00000000
    irq_hw_err_mod_mask          0xe0004150 = 0x00000000
    tst_ctrl                     0xe0004158 = 0x00000001
    gp_io                        0xe000415c = 0x0000000f
    i2c_ctrl                     0xe0004160 = 0x00000000
    i2c_data                     0xe0004164 = 0x00000000
    i2c_irq                      0xe0004168 = 0x00000000
    i2c_sw                       0xe000416c = 0x00000003

   RAM Random Registers:
    ram_addr                     0xe0004180 = 0x00000000
    ram_data_port_lo             0xe0004184 = 0x00000000
    ram_data_port_hi             0xe0004188 = 0x00000000

   Ram Interface Registers:
    ram_if_to_lo                 0xe0004190 = 0x24242424
    ram_if_to_hi                 0xe0004194 = 0x00002424
    ram_if_timeout_val           0xe000419c = 0x00000000
    ram_if_ctrl                  0xe00041a0 = 0x000a0002

   Transmit Arbiter MAC:
    tx_arb_iti_init              0xe0004200 = 0x00000000
    tx_arb_iti_val               0xe0004204 = 0x00000000
    tx_arb_lim_init              0xe0004208 = 0x00000000
    tx_arb_lim_val               0xe000420c = 0x00000000
    tx_arb_ctrl_tst_status       0xe0004210 = 0x00001256

   Bank 8: Receive queue registers:
    rx_qregs.buf_ctrl            0xe0004400 = 0xc8550800
    rx_qregs.next_desc_addr_lo   0xe0004404 = 0x016d4020
    rx_qregs.buf_addr_lo         0xe0004408 = 0x019acd00
```

```
 rx_qregs.buf_addr_hi          0xe000440c = 0x00000000
 rx_qregs.frame_sw             0xe0004410 = 0x00000000
 rx_qregs.time_stamp           0xe0004414 = 0x00000000
 rx_qregs.tcp_csum             0xe0004418 = 0x00000000
 rx_qregs.tcp_csum_start       0xe000441c = 0x00000000
 rx_qregs.desc_addr_lo         0xe0004420 = 0x016d4000
 rx_qregs.desc_addr_hi         0xe0004424 = 0x00000000
 rx_qregs.addr_cntr_lo         0xe0004428 = 0x016d4020
 rx_qregs.addr_cntr_hi         0xe000442c = 0x00000000
 rx_qregs.byte_cntr            0xe0004430 = 0x00000000
 rx_qregs.bmu_cs               0xe0004434 = 0x002aaa80
 rx_qregs.flag                 0xe0004438 = 0x00000600
 rx_qregs.tst1                 0xe000443c = 0xd2020202
 rx_qregs.tst2                 0xe0004440 = 0x00000050
 rx_qregs.tst3                 0xe0004444 = 0x00000000

Bank 12: Synchronous transmit queue registers:
 stx_qregs.buf_ctrl            0xe0004600 = 0x00000000
 stx_qregs.next_desc_addr_lo   0xe0004604 = 0x00000000
 stx_qregs.buf_addr_lo         0xe0004608 = 0x00000000
 stx_qregs.buf_addr_hi         0xe000460c = 0x00000000
 stx_qregs.frame_sw            0xe0004610 = 0x00000000
 stx_qregs.time_stamp          0xe0004614 = 0x00000000
 stx_qregs.tcp_csum            0xe0004618 = 0x00000000
 stx_qregs.tcp_csum_start      0xe000461c = 0x00000000
 stx_qregs.desc_addr_lo        0xe0004620 = 0x00000000
 stx_qregs.desc_addr_hi        0xe0004624 = 0x00000000
 stx_qregs.addr_cntr_lo        0xe0004628 = 0x00000000
 stx_qregs.addr_cntr_hi        0xe000462c = 0x00000000
 stx_qregs.byte_cntr           0xe0004630 = 0x00000000
 stx_qregs.bmu_cs              0xe0004634 = 0x01155540
 stx_qregs.flag                0xe0004638 = 0x0a000600
 stx_qregs.tst1                0xe000463c = 0x02020202
 stx_qregs.tst2                0xe0004640 = 0x00000050
 stx_qregs.tst3                0xe0004644 = 0x00000000

Bank 13: Asynchronous transmit queue registers:
 atx_qregs.buf_ctrl            0xe0004680 = 0x00000000
 atx_qregs.next_desc_addr_lo   0xe0004684 = 0x00000000
 atx_qregs.buf_addr_lo         0xe0004688 = 0x00000000
 atx_qregs.buf_addr_hi         0xe000468c = 0x00000000
 atx_qregs.frame_sw            0xe0004690 = 0x00000000
 atx_qregs.time_stamp          0xe0004694 = 0x00000000
 atx_qregs.tcp_csum            0xe0004698 = 0x00000000
 atx_qregs.tcp_csum_start      0xe000469c = 0x00000000
 atx_qregs.desc_addr_lo        0xe00046a0 = 0x016d9000
 atx_qregs.desc_addr_hi        0xe00046a4 = 0x00000000
 atx_qregs.addr_cntr_lo        0xe00046a8 = 0x016d901c
 atx_qregs.addr_cntr_hi        0xe00046ac = 0x00000000
 atx_qregs.byte_cntr           0xe00046b0 = 0x00000000
 atx_qregs.bmu_cs              0xe00046b4 = 0x012aaa80
 atx_qregs.flag                0xe00046b8 = 0x0a000600
 atx_qregs.tst1                0xe00046bc = 0x02020202
 atx_qregs.tst2                0xe00046c0 = 0x00000050
 atx_qregs.tst3                0xe00046c4 = 0x00000000

Bank 16: Receive RAM buffer registers:
 rx_ram_buf_regs.start_addr    0xe0004800 = 0x00000000
 rx_ram_buf_regs.end_addr      0xe0004804 = 0x000017ff
 rx_ram_buf_regs.wr_ptr        0xe0004808 = 0x00000000
 rx_ram_buf_regs.rd_ptr        0xe000480c = 0x00000000
 rx_ram_buf_regs.up_thres_pp   0xe0004810 = 0x00001400
 rx_ram_buf_regs.lo_thres_pp   0xe0004814 = 0x00001000
 rx_ram_buf_regs.up_thres_hp   0xe0004818 = 0x00000000
```

```
 rx_ram_buf_regs.lo_thres_hp   0xe000481c = 0x00000000
 rx_ram_buf_regs.pak_cnt       0xe0004820 = 0x00000000
 rx_ram_buf_regs.level         0xe0004824 = 0x00000000
 rx_ram_buf_regs.ctrl          0xe0004828 = 0x0002222a

Bank 20: Synchronous transmit RAM buffer registers:
 stx_ram_buf_regs.start_addr   0xe0004a00 = 0x00000000
 stx_ram_buf_regs.end_addr     0xe0004a04 = 0x00000000
 stx_ram_buf_regs.wr_ptr       0xe0004a08 = 0x00000000
 stx_ram_buf_regs.rd_ptr       0xe0004a0c = 0x00000000
 stx_ram_buf_regs.pak_cnt      0xe0004a20 = 0x00000000
 stx_ram_buf_regs.level        0xe0004a24 = 0x00000000
 stx_ram_buf_regs.ctrl         0xe0004a28 = 0x00022215

Bank 21: Asynchronous transmit RAM buffer registers:
 atx_ram_buf_regs.start_addr   0xe0004a80 = 0x00001800
 atx_ram_buf_regs.end_addr     0xe0004a84 = 0x00002fff
 atx_ram_buf_regs.wr_ptr       0xe0004a88 = 0x00001800
 atx_ram_buf_regs.rd_ptr       0xe0004a8c = 0x00001800
 atx_ram_buf_regs.up_thres_pp  0xe0004a90 = 0x00000000
 atx_ram_buf_regs.lo_thres_pp  0xe0004a94 = 0x00000000
 atx_ram_buf_regs.up_thres_hp  0xe0004a98 = 0x00000000
 atx_ram_buf_regs.lo_thres_hp  0xe0004a9c = 0x00000000
 atx_ram_buf_regs.pak_cnt      0xe0004aa0 = 0x00000000
 atx_ram_buf_regs.level        0xe0004aa4 = 0x00000000
 atx_ram_buf_regs.ctrl         0xe0004aa8 = 0x0002222a

Bank 24: Receive GMAC FIFO registers:
 rx_gmfifo_regs.end_addr       0xe0004c40 = 0x0000007f
 rx_gmfifo_regs.thr            0xe0004c44 = 0x00000070
 rx_gmfifo_regs.ctrl           0xe0004c48 = 0x0000224a

Bank 26: Transmit GMAC FIFO registers:
 tx_gmfifo_regs.end_addr       0xe0004d40 = 0x0000007f
 tx_gmfifo_regs.thr            0xe0004d44 = 0x00000010
 tx_gmfifo_regs.ctrl           0xe0004d48 = 0x0002220a
 tx_gmfifo_regs.wr_ptr         0xe0004d60 = 0x00000000
 tx_gmfifo_regs.wr_shdw_ptr    0xe0004d64 = 0x00000000
 tx_gmfifo_regs.wr_level       0xe0004d68 = 0x00000000
 tx_gmfifo_regs.rd_ptr         0xe0004d70 = 0x00000000
 tx_gmfifo_regs.restart_ptr    0xe0004d74 = 0x00000000
 tx_gmfifo_regs.rd_level       0xe0004d78 = 0x00000000

Descriptor poll timer registers:
 dpt_init_val                  0xe0004e00 = 0x00000000
 dpt_val                       0xe0004e04 = 0x00000000
 dpt_ctrl                      0xe0004e08 = 0x00020001

Timestamp timer register:
 ts_timer_val                  0xe0004e14 = 0x00000000
 ts_timer_ctrl                 0xe0004e18 = 0x00000202

GMAC and GPHY control registers:
 gmac_ctrl                     0xe0004f00 = 0x00000056
 gphy_ctrl                     0xe0004f04 = 0x0b7de002
 gmac_irq_src                  0xe0004f08 = 0x00000000
 gmac_irq_msk                  0xe0004f0c = 0x0000003a
 gmac_link_ctrl                0xe0004f10 = 0x00000002

Wake on LAN control registers:
 wol_ctrl                      0xe0004f20 = 0x00000555
 wol_mac_addr_lo               0xe0004f24 = 0x00000000
 wol_mac_addr_hi               0xe0004f28 = 0x00000000
 wol_patt_rd_ptr               0xe0004f2c = 0x00000000
```

```
    wol_patt_len_lo               0xe0004f30 = 0x3b3b3b3b
    wol_patt_len_hi               0xe0004f34 = 0x003b3b3b
    wol_patt_cnt_lo               0xe0004f38 = 0x00000000
    wol_patt_cnt_hi               0xe0004f3c = 0x00000000

   Bank 80 (0x50): GMAC registers:
    gmac_gpsr                     0xe0006800 = 0x0000f014
    gmac_gpcr                     0xe0006804 = 0x000038ff
    gmac_tx_ctrl                  0xe0006808 = 0x00001c00
    gmac_rx_ctrl                  0xe000680c = 0x0000a000
    gmac_tx_fctrl                 0xe0006810 = 0x0000ffff
    gmac_tx_parm                  0xe0006814 = 0x0000c000
    gmac_smod                     0xe0006818 = 0x00002306
    gmac_sa1_lo                   0xe000681c = 0x0000d000
    gmac_sa1_md                   0xe0006820 = 0x0000ff2b
    gmac_sa1_hi                   0xe0006824 = 0x00009f44
    gmac_sa2_lo                   0xe0006828 = 0x0000d000
    gmac_sa2_md                   0xe000682c = 0x0000ff2b
    gmac_sa2_hi                   0xe0006830 = 0x00009f44
    gmac_mcast_addr_hash1         0xe0006834 = 0x00000000
    gmac_mcast_addr_hash2         0xe0006838 = 0x00000000
    gmac_mcast_addr_hash3         0xe000683c = 0x00000000
    gmac_mcast_addr_hash4         0xe0006840 = 0x00000000
    gmac_tx_irq_src               0xe0006844 = 0x00000000
    gmac_rx_irq_src               0xe0006848 = 0x00000000
    gmac_tr_irq_src               0xe000684c = 0x00000000
    gmac_tx_irq_msk               0xe0006850 = 0x00000000
    gmac_rx_irq_msk               0xe0006854 = 0x00000000
    gmac_tr_irq_msk               0xe0006858 = 0x00000000

Internal-Data0/1:
   Marvell 88E6095 revision 2, switch port 8
     Port Registers:
         Status:        0x0e84  PCS Ctrl:      0xc13e
         Identifier:    0x0952  Port Ctrl:     0x0177
         Port Ctrl-1:   0x0000  Vlan Map:      0x06ff
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0100
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
```

次に、**show controller detail** コマンドの出力例を示します。

```
hostname# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
```

```
    RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
    RX Descriptor 0 Length:     0xf8262808 = 0x00001000
    RX Descriptor 0 Head:       0xf8262810 = 0x00000000
    RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
    RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
    RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
    RX Descriptor 1 Length:     0xf8260140 = 0x00000000
    RX Descriptor 1 Head:       0xf8260148 = 0x00000000
    RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

TX Descriptor Registers:
    TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
    TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
    TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
    TX Descriptor 0 Length:     0xf8263808 = 0x00001000
    TX Descriptor 0 Head:       0xf8263810 = 0x00000000
    TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

RX Address Array:
    Ethernet Address 0:         0012.d948.ef58
    Ethernet Address 1:         Not Valid!
    Ethernet Address 2:         Not Valid!
    Ethernet Address 3:         Not Valid!
    Ethernet Address 4:         Not Valid!
    Ethernet Address 5:         Not Valid!
    Ethernet Address 6:         Not Valid!
    Ethernet Address 7:         Not Valid!
    Ethernet Address 8:         Not Valid!
    Ethernet Address 9:         Not Valid!
    Ethernet Address a:         Not Valid!
    Ethernet Address b:         Not Valid!
    Ethernet Address c:         Not Valid!
    Ethernet Address d:         Not Valid!
    Ethernet Address e:         Not Valid!
    Ethernet Address f:         Not Valid!

PHY Registers:
    Phy Control:                0x1140
    Phy Status:                 0x7969
    Phy ID 1:                   0x0141
    Phy ID 2:                   0x0c25
    Phy Autoneg Advertise:      0x01e1
    Phy Link Partner Ability:   0x41e1
    Phy Autoneg Expansion:      0x0007
    Phy Next Page TX:           0x2801
    Phy Link Partnr Next Page:  0x0000
    Phy 1000T Control:          0x0200
    Phy 1000T Status:           0x4000
    Phy Extended Status:        0x3000

Detailed Output - RX Descriptor Ring:

rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

........
```

関連コマンド

コマンド	説明
show interface	インターフェイス統計情報を表示します。
show tech-support	Cisco TAC による問題の診断を可能にするような情報を表示します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

構文の説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、すべてのカウンタを表示する例を示します。

```
hostname# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

hostname# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
```

次に、カウンタの要約を表示する例を示します。

```
hostname# show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

次に、コンテキストのカウンタを表示する例を示します。

```
hostname# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu** コマンドを使用します。

show cpu [**usage | profile | detailed**]

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

show cpu [**usage**] [**context** {**all** | *context_name*}]

構文の説明

all	すべてのコンテキストを表示することを指定します。
context	1 つのコンテキストを表示することを指定します。
context_name	表示するコンテキストの名前を指定します。
detailed	（任意）CPU の内部使用に関する詳細な情報を表示します。
profile	（任意）CPU のプロファイリング データを表示します。
usage	（任意）CPU 使用状況を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

CPU の使用状況は、5 秒ごとの負荷の近似値を使用し、この概算値をさらに以降の 2 つの移動平均に適用することによって算出されます。

show cpu コマンドを使用すると、プロセス関連の負荷を検出できます（つまり、**show process** コマンドを、シングルモードとマルチ コンテキスト モードのシステム コンフィギュレーションの両方で実行した場合に表示される項目の代わりに、アクティビティを表示できます）。

さらに、マルチ コンテキスト モードでは、プロセス関連負荷を分散するよう、設定されたすべてのコンテキストで消費される CPU に要求できます。このためには、各コンテキストに変更して **show cpu** コマンドを入力するか、このコマンドのバリアントである **show cpu context** を入力します。

プロセス関連の負荷は、最も近い整数に丸められますが、コンテキスト関連の負荷の場合は精度を表す 10 進数が 1 つ追加されます。たとえば、**show cpu** をシステム コンテキストから入力すると、**show cpu context system** コマンドを入力したときとは別の数値が示されます。前者は **show cpu context all** の要約とほぼ同じですが、後者はその要約の一部にすぎません。

show cpu profile コマンドと、cpu profile activate コマンドを併用することで、CPU の問題の修復を支援するために TAC が収集および使用できる情報を表示できます。show cpu profile コマンドによって表示される情報は 16 進数です。

例

次に、CPU 使用状況を表示する例を示します。

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次に、マルチ モードでシステム コンテキストの CPU 使用状況を表示する例を示します。

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次に、すべてのコンテキストの CPU 使用状況を表示する例を示します。

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次に、「one」というコンテキストの CPU 使用状況を表示する例を示します。

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

次の例では、プロファイラが稼働し、5000 個のサンプルの格納が命令されます。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

結果を確認するには、**show cpu profile** コマンドを使用します。

（注） **cpu profile activate** コマンドの実行中に **show cpu profile** を実行すると、進捗が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

完了すると、**show cpu profile** コマンドの出力に結果が表示されます。この情報をコピーし、デコードする TAC に提供します。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000 samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d 002198af
0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPU プロファイリングをアクティブにします。

show crashinfo

フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示するには、特権 EXEC モードで **show crashinfo** コマンドを使用します。

show crashinfo [**save**]

構文の説明

save	（任意）クラッシュ情報をフラッシュ メモリに保存するようにセキュリティ アプライアンスが設定されているかどうかを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンドで生成）である場合、クラッシュ ファイルの最初のストリングは「**: Saved_Test_Crash**」であり、最後のストリングは「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュである場合、クラッシュ ファイルの最初の行の文字列は「**: Saved_Crash**」で、最後の文字列は「**: End_Crash**」です。（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データをクリアしていた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

例

次に、現在のクラッシュ情報コンフィギュレーションを表示する例を示します。

```
hostname# show crashinfo save
crashinfo save enable
```

次に、クラッシュ ファイル テストの出力例を示します（このテストによって、セキュリティ アプライアンスが実際にクラッシュすることはありません。このテストで提供されるのは、シミュレートされたサンプル ファイルです）。

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
```

```
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
```

```
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
```

```
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
```

```
This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
```

```
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
```

```
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。

show crashinfo console

crashinfo console コマンドのコンフィギュレーション設定を表示するには、**show crashinfo console** コマンドを入力します。

show crashinfo console

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 140-2 に準拠していることにより、キーやパスワードなどのクリティカル セキュリティ パラメータをクリプト境界（シャーシ）の外側に配布することが禁止されています。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域には、機密データが含まれていることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

show crypto accelerator statistics

ハードウェア クリプト アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

出力統計情報は、次のように定義されます。

アクセラレータ 0 はソフトウェアベースのクリプト エンジンです。

アクセラレータ 1 はハードウェアベースのクリプト エンジンです。

RSA 統計情報には、ソフトウェアでのみ実行される、2048 ビット キーの RSA 処理が表示されます。つまり、2048 ビット キーがある場合、IKE/SSL VPN は、IPSec/SSL ネゴシエーション フェーズ中にソフトウェアで RSA 処理を実行します。実際の IPSec/SSL トラフィックは、引き続きハードウェアを使用して処理されます。これにより、同時に開始された同時セッションが数多くある場合、CPU の高使用となります。このため、RSA キー処理が複数発生し、CPU の高使用となる可能性があります。このようにして CPU の高使用状態となった場合は、1024 ビット キーを使用して、ハードウェアで RSA キー処理を実行する必要があります。このためには、アイデンティティ証明書を再度登録する必要があります。

2048 ビットの RSA キーを使用しており、ソフトウェアで RSA 処理が実行されている場合は、CPU プロファイリングを使用して、CPU の高使用状況の原因となっている関数を特定できます。通常、bn_* 関数と BN_* 関数は RSA に使用される大規模なデータ セットでの数学的処理であり、ソフトウェアでの RSA 処理中に CPU の使用状況を確認する場合に最も役立ちます。次に例を示します。

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 統計情報には、ソフトウェアで 1024 より大きいモジュラス サイズの暗号処理が実行されたことが表示されます（DH5（Diffie-Hellman グループ 5 が 1536 を使用しています）など）。この場合、2048 ビット キー証明書はソフトウェアで処理されます。このため、数多くのセッションが実行されるときに CPU の高使用状況となります。

（注）　ASA 5580（Cavium クリプト チップ搭載）のみが、ハードウェアにより高速化される 2048 ビットの RSA キー生成をサポートしています。ASA 5510、5520、5540、および 5550 は、ハードウェアにより高速化される 2048 ビットのキー生成をサポートしていません。ASA 5505（Cavium CN505 プロセッサ搭載）のみが、ハードウェアにより高速化される 768 ビットおよび 1024 ビットのキー生成の Diffie-Hellman グループ 1 および 2 をサポートしています。Diffie-Hellman グループ 5（1536 ビットのキー生成）は、ソフトウェアで実行されます。

適応型セキュリティ アプライアンスでは 1 つのクリプト エンジンが IPSec 処理および SSL 処理を実行します。起動時にハードウェア クリプト アクセラレータにロードされたクリプト（Cavium）マイクロコードのバージョンを表示するには、**show version** コマンドを入力します。次に例を示します。

```
hostname(config) show version

Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is “disk0:/interim/asa804-8-k8.bin”
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 統計情報には、2 つのフェーズでのキー生成が表示されます。最初のフェーズは、アルゴリズム パラメータの選択です。このパラメータは、システムの他のユーザと共有することがあります。2 番めのフェーズは、1 人のユーザ用の秘密キーと公開キーの算出です。

SSL 統計情報には、ハードウェア クリプト アクセラレータへの SSL トランザクションで使用される、プロセッサ集約的な公開キーの暗号化アルゴリズムに関するレコードが表示されます。

RNG 統計情報には、キーとして使用する同じ乱数のセットを自動的に生成できる送信元とレシーバに関するレコードが表示されます。

例

次に、グローバル コンフィギュレーション モードでグローバルなクリプト アクセラレータ統計情報を表示する例を示します。

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
```

```
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
```

```
   Decrypted packets: 700
   Decrypted bytes: 719944
[Output statistics]
   Output packets: 700
   Output bad packets: 0
   Output bytes: 767552
   Output hashed packets: 700
   Output hashed bytes: 744800
   Encrypted packets: 700
   Encrypted bytes: 728352
[Diffie-Hellman statistics]
   Keys generated: 97
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
   Encrypted packets: 0
   Encrypted bytes: 0
   Decrypted packets: 0
   Decrypted bytes: 0
[DSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 0
   Inbound records: 0
[RNG statistics]
   Random number requests: 1
   Random number request failures: 0
```

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
Capacity	このセクションは、セキュリティ アプライアンスがサポートできるクリプト アクセラレーションに関連しています。
Supports hardware crypto	(True/False）セキュリティ アプライアンスはハードウェア クリプト アクセラレーションをサポートできます。
Supports modular hardware crypto	(True/False）サポートされている任意のハードウェア クリプト アクセラレータを個別のプラグイン カードまたはモジュールとして挿入できます。
Max accelerators	セキュリティ アプライアンスでサポートされるハードウェア クリプト アクセラレータの最大数。
Mac crypto throughput	セキュリティ アプライアンスの最大定格 VPN スループット。
Max crypto connections	セキュリティ アプライアンスのサポート対象 VPN トンネルの最大数。
Global Statistics	このセクションは、セキュリティ アプライアンスの複合ハードウェア クリプト アクセラレータに関連しています。
Number of active accelerators	アクティブなハードウェア アクセラレータの数。アクティブなハードウェア アクセラレータが初期化されており、crypto コマンドの処理に使用可能です。

出力 （続き）	説明 （続き）
Number of non-operational accelerators	非アクティブなハードウェア アクセラレータの数。非アクティブなハードウェア アクセラレータが検出されました。初期化が完了していないか、障害が発生して使用できなくなっています。
Input packets	すべてのハードウェア クリプト アクセラレータで処理される着信パケットの数。
Input bytes	処理される着信パケット内のデータのバイト数。
Output packets	すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output error packets	エラーが検出された、すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output bytes	処理される発信パケット内のデータのバイト数。
Accelerator 0	各セクションは、クリプト アクセラレータに関連しています。最初のセクション（Accelerator 0）は、常に、ソフトウェア クリプト エンジンです。ハードウェア アクセラレータではありませんが、セキュリティ アプライアンスはこのソフトウェア クリプト エンジンを使用して、特定のクリプト タスクを実行します。ここには、その統計情報が表示されます。Accelerators 1 以上は、常に、ハードウェア クリプト アクセラレータです。
Status	アクセラレータのステータス。アクセラレータが初期化されているか、アクティブか、あるいは失敗したかを示します。
Software crypto engine	アクセラレータのタイプとファームウェア バージョン（該当する場合）。
Slot	アクセラレータのスロット番号（該当する場合）。
Active time	アクセラレータがアクティブ状態であった時間の長さ。
Total crypto transforms	アクセラレータによって実行された crypto コマンドの合計数。
Total dropped packets	エラーのためアクセラレータによってドロップされたパケットの合計数。
Input statistics	このセクションは、アクセラレータで処理された入力トラフィックに関連しています。入力トラフィックは、複合か認証、またはその両方を行う必要がある暗号文と見なされます。
Input packets	アクセラレータによって処理された入力パケットの数。
Input bytes	アクセラレータによって処理された入力バイト数。
Input hashed packets	アクセラレータがハッシュを実行したパケットの数。
Input hashed bytes	アクセラレータがハッシュを実行したバイト数。
Decrypted packets	アクセラレータが対称復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが対称復号化を実行したバイト数。
Output statistics	このセクションは、アクセラレータで処理された出力トラフィックに関連しています。入力トラフィックは、暗号化かハッシュ、またはその両方を実行する必要があるクリア テキストと見なされます。
Output packets	アクセラレータによって処理された出力パケットの数。

出力 （続き）	説明 （続き）
Output bad packets	エラーが検出された、アクセラレータで処理された出力パケットの数。
Output bytes	アクセラレータによって処理された出力バイト数。
Output hashed packets	アクセラレータが出力ハッシュを実行したパケットの数。
Output hashed bytes	アクセラレータが出力ハッシュを実行したバイト数。
Encyrpted packets	アクセラレータが対称暗号化を実行したパケットの数。
Encyrpted bytes	アクセラレータが対称暗号化を実行したバイト数。
Diffie-Hellman statistics	このセクションは、Diffie-Hellman のキー交換処理に関連しています。
Keys generated	アクセラレータによって生成された Diffie-Hellman キー セットの数。
Secret keys derived	アクセラレータによって生成された Diffie-Hellman 共有秘密の数。
RSA statistics	このセクションは、RSA 暗号処理に関連しています。
Keys generated	アクセラレータによって生成された RSA キー セットの数。
Signatures	アクセラレータによって実行された RSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された RSA シグニチャ確認の数。
Encrypted packets	アクセラレータが RSA 暗号化を実行したパケットの数。
Decrypted packets	アクセラレータが RSA 復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが RSA 復号化を実行したデータのバイト数。
DSA statistics	このセクションは、DSA 処理に関連しています。DSA はバージョン 8.2 以上ではサポートされないため、この統計情報は表示されません。
Keys generated	アクセラレータによって生成された DSA キー セットの数。
Signatures	アクセラレータによって実行された DSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された DSA シグニチャ確認の数。
SSL statistics	このセクションは、SSL レコード処理に関連しています。
Outbound records	アクセラレータによって暗号化され、認証された SSL レコードの数。
Inbound records	アクセラレータによって復号化され、認証された SSL レコードの数。
RNG statistics	このセクションは、乱数生成に関連しています。
Random number requests	アクセラレータに対する乱数の要求の数。
Random number request failures	アクセラレータに対する乱数要求のうち、失敗した要求の数。

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合は、システムにインストールされているすべての証明書が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、tp1 というトラストポイントの CA 証明書を表示する例を示します。

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
```

```
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント モードを開始します。

show crypto ca crls

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合は、システムにキャッシュされているすべての CRL が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、tp1 というトラストポイントの CRL を表示する例を示します。

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。

コマンド	説明
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント モードを開始します。

show crypto ca server

セキュリティ アプライアンスにあるローカル Certificate Authority（CA; 認証局）コンフィギュレーションのステータスを表示するには、**show crypto ca server** コマンドを使用します。

show crypto ca server

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、ローカル CA サーバのすべてのコンフィギュレーション データのステータスを表示する例を示します。

```
hostname# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
    Current primary storage dir: nvram:
hostname#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server certificate	ローカル CA の証明書を Base-64 形式で表示します。
show crypto ca server crl	ローカル CA CRL のライフタイムを表示します。

show crypto ca server cert-db

特定のユーザに対して発行される証明書を含め、ローカル Certificate Authority（CA; 認証局）サーバのすべての証明書、またはそのサブセットを表示するには、**show crypto ca server cert-db** コマンドを使用します。

show crypto ca server cert-db [user *username* **| allowed | enrolled | expired | on-hold]**

[serial *certificate-serial-number*]

構文の説明

allowed	証明書のステータスに関係なく、登録を許可されているユーザを表示するように指定します。
enrolled	有効な証明書を持つユーザを表示するように指定します。
expired	期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	まだ登録されていないユーザを表示するように指定します。
serial *certificate-serial-number*	表示する特定の証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。
user **username**	証明書の所有者を指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。

デフォルト

デフォルトでは、ユーザ名や証明書のシリアル番号が指定されていない場合は、発行された証明書のデータベース全体が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show crypto ca server cert-db コマンドは、ローカル CA サーバによって発行されたユーザ証明書のリストを表示します。1 つ以上の証明書タイプ キーワードをオプションとして付けて、またはオプションの証明書シリアル番号を付けて、特定のユーザ名を指定し、証明書データベースのサブセットを表示できます。

キーワードまたはシリアル番号なしでユーザ名を指定すると、そのユーザに対して発行された証明書がすべて表示されます。ユーザごとに、ユーザ名、*renewal allowed till* フィールド、*number of times the user is notified* カウント、および *PKCS12 file stored till* 値が、そのユーザに対して発行された証明書の前に表示されます。

それぞれの証明書には、証明書のシリアル番号、発行日付と有効期限日付、および証明書のステータス（Revoked/Not Revoked）が表示されます。

例

次に、CA サーバが Janedoe に対して発行した証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db user janedoe
```

次に、ローカル CA サーバによって発行された、シリアル番号が 0x100 以上の証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db serial 1oo
```

次に、ローカル CA サーバによって発行された証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server revoke	証明書データベースと Certificate Revocation List（CRL; 証明書失効リスト）の両方で、ローカル CA サーバによって発行された証明書を失効としてマークします。
lifetime crl	証明書失効リストのライフタイムを指定します。

show crypto ca server certificate

ローカル Certificate Authority（CA; 認証局）サーバの証明書を Base-64 形式で表示するには、**show crypto ca server certificate** コマンドを使用します。

show crypto ca server certificate

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show crypto ca server certificate コマンドにより、ローカル CA サーバの証明書が Base-64 形式で表示されます。これで、ローカル CA サーバを信頼する必要がある他のデバイスに証明書をエクスポートするときに、その証明書をカット アンド ペーストできます。

例

次に、ローカル CA サーバのサーバ証明書を表示する例を示します。

```
hostname# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34ql1NE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

hostname#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA コンフィギュレーションを ASCII テキスト形式で表示します。

show crypto ca server crl

ローカル Certificate Authority（CA; 認証局）の現在の Certificate Revocation List（CRL; 証明書失効リスト）を表示するには、**show crypto ca server crl** コマンドを表示します。

show crypto ca server crl

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、組み込み CA サーバの現在の CRL を表示する例を示します。

```
hostname# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
hostname#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める、Certificate Revocation List（CRL; 証明書失効リスト）の Distribution Point（CDP; 配布ポイント）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。

コマンド	説明
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
lifetime crl	Certificate Revocation List（CRL; 証明書失効リスト）のライフタイムを指定します。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

show crypto ca server user-db

ローカル Certificate Authority（CA; 認証局）サーバのユーザ データベースに存在するユーザを表示するには、**show crypto ca server user-db** コマンドを使用します。

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

構文の説明

allowed	（任意）証明書のステータスに関係なく、登録を許可されたユーザを表示するように指定します。
enrolled	（任意）有効な証明書を持つユーザを表示するように指定します。
expired	（任意）期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	（任意）まだ登録されていないユーザを表示するように指定します。

デフォルト

デフォルトでは、キーワードが入力されない場合にはデータベース内のすべてのユーザが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、現在登録されているユーザを表示する例を示します。

```
hostname# crypto ca server user-db enrolled
Username    DN                 Certificate issued    Certificate expiration
jandoe      cn=Jan Doe,o=...   5/31/2006             5/31/2007

hostname#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
crypto ca server user-db write	ローカル CA データベースで設定されているユーザ情報をストレージに書き込みます。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

show crypto debug-condition

IPSec および ISAKMP のデバッグ メッセージに対して現在設定されているフィルタ、一致しない状態、およびエラー ステートを表示するには、グローバル コンフィギュレーション モードで **show crypto debug-condition** コマンドを使用します。

show crypto debug-condition

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、フィルタリング条件を表示する例を示します。

```
hostname(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPSec debug context unmatched flag:  ON

IKE peer IP address filters:
1.1.1.0/24   2.2.2.2

IKE user name filters:
my_user
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットの IPSec DF-bit ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、inside というインターフェイスの IPSec DF-bit ポリシーを表示する例を示します。

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF-bit ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、inside というインターフェイスの IPSec フラグメンテーション ポリシーを表示する例を示します。

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec sa** コマンドを使用します。このコマンドの別の形式である **show ipsec sa** を使用することもできます。

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

detail	（任意）表示されているものに対する詳細なエラー情報を表示します。
entry	（任意）IPSec SA をピア アドレスの順に表示します。
identity	（任意）IPSec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	（任意）指定されたクリプト マップの IPSec SA を表示します。
peer *peer-addr*	（任意）指定されたピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec SA が表示されます。

```
hostname(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

（注） IPSec SA ポリシーに、フラグメンテーションは IPSec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーで、フラグメンテーションは IPSec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次の例をグローバル コンフィギュレーション モードで入力すると、def という名前のクリプト マップの IPSec SA が表示されます。

```
hostname(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
```

```
          IV size: 8 bytes
          replay detection support: Y
      outbound esp sas:
        spi: 0xDC15BF68 (3692412776)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 480
          IV size: 8 bytes
          replay detection support: Y

      Crypto map tag: def, local addr: 172.20.0.17

        local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
        current_peer: 10.135.1.8
        dynamic allocated peer ip: 0.0.0.0

        #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
        #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
        #send errors: 0, #recv errors: 0

        local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

        path mtu 1500, ipsec overhead 60, media mtu 1500
        current outbound spi: 3B6F6A35

      inbound esp sas:
        spi: 0xB32CF0BD (3006066877)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 263
          IV size: 8 bytes
          replay detection support: Y
      outbound esp sas:
        spi: 0x3B6F6A35 (997157429)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 263
          IV size: 8 bytes
          replay detection support: Y
hostname(config)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry** に対する IPSec SA が表示されます。

```
hostname(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry detail** を使って、IPSec SA が表示されます。

```
hostname(config)# show crypto ipsec sa entry detail
```

```
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
```

```
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次に、キーワード **identity** を使った IPSec SA の例を示します。

```
hostname(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使った IPSec SA の例を示します。

```
hostname(config)# show crypto ipsec sa identity detail
```

```
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

IPSec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
hostname(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
```

```
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPSec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが非推奨コマンドになりました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE ピア	タイプ	Dir	Rky	ステート
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE ピア	タイプ	Dir	Rky	ステート	暗号	ハッシュ	認証	ライフタイム
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
hostname(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが非推奨コマンドになりました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

構文の説明

protocol	統計情報を表示するプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 **ikev1**：インターネット キー交換バージョン 1。 **ipsec**：IP セキュリティ フェーズ 2 プロトコル。 **ssl**：Secure Socket Layer。 **other**：新規プロトコル用に予約済み。 **all**：現在サポートされているすべてのプロトコル。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、指定したプロトコルに関するクリプト アクセラレータ統計情報を表示する例を示します。

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
```

```
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
```

```
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。

show csc node-count

ノードとは、固有の送信元 IP アドレス、またはセキュリティ アプライアンスにより保護されているネットワーク上のデバイスのアドレスです。セキュリティ アプライアンスは、毎日のノード カウントを追跡し、ユーザ ライセンスの強制のために CSC SSM に伝えます。CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

show csc node-count [**yesterday**]

構文の説明

yesterday	（任意）CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示します。

デフォルト

デフォルトで表示されるノード カウントは、午前 0 時からスキャンされたノード数です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show csc node-count** コマンドを使用して、CSC SSM が午前 0 時からスキャンしたトラフィックのノード数を表示する例を示します。

```
hostname# show csc node-count
Current node count is 1
```

次に、**show csc node-count** コマンドを使用して、CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示する例を示します。

```
hostname(config)# show csc node-count yesterday
Yesterday's node count is 2
```

関連コマンド

csc	ネットワーク トラフィックを CSC SSM に送信して、CSC SSM で設定されているとおりに FTP、HTTP、POP3、および SMTP をスキャンします。
show running-config class-map	現在のクラス マップ コンフィギュレーションを表示します。

show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス ポリシー コンフィギュレーションを表示します。

show ctiqbe

セキュリティ アプライアンスを越えて確立された CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show ctiqbe コマンドは、セキュリティ アプライアンスを越えて確立された CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** とともに、このコマンドは、CTIQBE インスペクション エンジンの問題のトラブルシューティングに使用されます。

（注） **show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンスを越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# show ctiqbe

Total: 1
  LOCAL  FOREIGN  STATE  HEARTBEAT
------------------------------------------------------------
1  10.0.0.99/1117   172.29.1.77/2748  1  120
  RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028  1029)
  MEDIA: Device ID 27  Call ID 0
  Foreign 172.29.1.99  (1028  1029)
```

```
|Local|172.29.1.88|(26822|26823)
|-----------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル）受信ポートは UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
hostname#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように変更されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次に、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力例を示します。ユーザ名はログイン時にユーザが入力した名前を示し、P_PRIV はユーザが **enable** コマンドを入力したことを示し、P_CONF はユーザが **config terminal** コマンドを入力したことを示します。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit
```

```
hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

次に、既知の動作を示します。次の例に示すように、イネーブル モードの場合は、ディセーブル モードを開始し、初期のログイン ユーザ名を enable_1 で置き換えます。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
asa2(config)# disable
asa2> show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show running-config privilege	コマンドの特権レベルを表示します。

CHAPTER 26

show ddns update interface コマンド～ show ipv6 traffic コマンド

show ddns update interface

セキュリティ アプライアンス インターフェイスに割り当てられた DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを使用します。

show ddns update interface [*interface-name*]

構文の説明

interface-name	（任意）ネットワーク インターフェイスの名前。

デフォルト

interface-name ストリングを省略すると、各インターフェイスに割り当てられている DDNS 方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、内部インターフェイスに割り当てられている DDNS 方式を表示する例を示します。

```
hostname# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
hostname#
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update method	設定済みの DDNS 方式ごとにタイプと間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show ddns update method

実行コンフィギュレーションの DDNS 更新方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

show ddns update method [*method-name***]**

構文の説明

method-name	（任意）設定済み DDNS 更新方式の名前。

デフォルト

method-name ストリングを省略すると、設定されているすべての DDNS 更新方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ddns-2 という名前の DDNS 方式を表示する例を示します。

```
hostname(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
hostname(config)#
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	セキュリティ アプライアンス インターフェイスを Dynamic DNS（DDNS; ダイナミック DNS）更新方式または DDNS 更新ホスト名に関連付けます。
ddns update method（**グローバル コンフィギュレーション モード**）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show debug

現在のデバッグ コンフィギュレーションを表示するには、**show debug** コマンドを使用します。

show debug [*command* [*keywords*]]

構文の説明

command	（任意）現在のコンフィギュレーションを表示する対象のデバッグ コマンドを指定します。各 *command* では、*command* の後の構文は、関連する **debug** コマンドでサポートされる構文と同一です。たとえば、**show debug aaa** の後に続く有効な *keywords* は、**debug aaa** コマンドの有効なキーワードと同じです。したがって、**show debug aaa** は **accounting** キーワードをサポートし、このキーワードによって AAA デバッグのその部分についてのデバッグ コンフィギュレーションを表示することを指定できます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	使用可能なコマンド値のリストに **eigrp** キーワードが追加されました。

使用上のガイドライン

有効な *command* 値が後に続きます。各 *command* では、*command* の後の構文は、関連する **debug** コマンドでサポートされる構文と同一です。サポートされている構文については、関連する **debug** コマンドを参照してください。

（注） 各 *command* 値を使用できるかどうかは、該当する **debug** コマンドをサポートするコマンド モードによって決まります。

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**

- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

例

次のコマンドでは、認証、アカウンティング、およびフラッシュ メモリのデバッグをイネーブルにします。**show debug** コマンドが 3 通りの方法で使用され、すべてのデバッグ コンフィギュレーション、特定機能のデバッグ コンフィギュレーション、機能のサブセットのデバッグ コンフィギュレーションを表示するためのコマンドの使用方法が示されています。

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
```

```
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
debug	すべての **debug** コマンドを参照してください。

show debug mmp

MMP インスペクション モジュールの現在のデバッグ設定を表示するには、特権 EXEC モードで **show debug mmp** コマンドを使用します。

show debug mmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、MMP インスペクション モジュールの現在のデバッグ設定を表示するために **show debug mmp** コマンドを使用する例を示します。

```
hostname# show debug mmp
debug mmp  enabled at level 1
```

関連コマンド

コマンド	説明
debug mmp	MMP イベントのインスペクションを表示します。
inspect mmp	MMP インスペクション エンジンを設定します。

show dhcpd

DHCP のバインディング情報、状態情報、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcpd** コマンドを使用します。

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

構文の説明

binding	所定のサーバ IP アドレスおよび関連するクライアント ハードウェア アドレスについてのバインディング情報とリースの長さを表示します。
IP_address	指定した IP アドレスのバインディング情報を表示します。
state	DHCP サーバの状態（現在のコンテキストでイネーブルかどうか、各インターフェイスについてイネーブルかどうかなど）を表示します。
statistics	統計情報（アドレス プール、バインディング、期限切れバインディング、不正な形式のメッセージ、送信済みメッセージ、および受信メッセージなどの数）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

オプションの IP アドレスを **show dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけが表示されます。

show dhcpd binding | state | statistics コマンドはグローバル コンフィギュレーション モードでも使用可能です。

例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

次に、**show dhcpd state** コマンドの出力例を示します。

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
```

```
Interface inside, Not Configured for DHCP
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
clear dhcpd	DHCP サーバ バインディングおよび統計情報カウンタをクリアします。
dhcpd lease	クライアントに付与される DHCP 情報のリースの長さを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

show dhcprelay state

DHCP リレー エージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

show dhcprelay state

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、現在のコンテキストおよび各インターフェイスについての DHCP リレー エージェントの状態情報を表示します。

例

次に、**show dhcprelay state** コマンドの出力例を示します。

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

関連コマンド

コマンド	説明
show dhcpd	DHCP サーバの統計情報と状態情報を表示します。
show dhcprelay statistics	DHCP リレーの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

show dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show dhcprelay statistics コマンドの出力は、**clear dhcprelay statistics** コマンドを入力するまで増加します。

例

次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
hostname#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェントの統計カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay state	DHCP リレー エージェントの状態を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

show disk

適応型セキュリティ アプライアンスのフラッシュ メモリの内容だけを表示するには、特権 EXEC モードで **show disk** コマンドを使用します。PIX セキュリティ アプライアンスのフラッシュ メモリの内容だけを表示するには、**show flash** コマンドを参照してください。

show disk[**0** | **1**] [**filesys** | **all**] **controller**

構文の説明

0	**1**	内部フラッシュ メモリ（0、デフォルト）または外部フラッシュ メモリ（1）を指定します。
controller	フラッシュ コントローラのモデル番号を指定します。
filesys	コンパクト フラッシュ カードの情報を表示します。
all	フラッシュ メモリの内容およびファイル システム情報を表示します。

デフォルト

デフォルトでは内部フラッシュ メモリを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show disk** コマンドの出力例を示します。

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
```

```
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

次に、**show disk filesys** コマンドの出力例を示します。

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

次に、**show disk controller** コマンドの出力例を示します。

```
hostname# show disk1: controller
Flash Model: TOSHIBA THNCF064MBA
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show flash	PIX セキュリティ アプライアンス専用の内部フラッシュ メモリの内容を表示します。

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバからダイナミックに学習したエントリと、**name** コマンドを使用して手動で入力された名前および IP アドレスが含まれています。

show dns-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show dns-hosts** コマンドの出力例を示します。

```
hostname# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

表 11 に、各フィールドの説明を示します。

表 26-1　show dns-hosts の各フィールド

フィールド	説明
Host	ホスト名を表示します。
Flags	次の組み合わせとしてエントリのステータスを表示します。 • temp：このエントリは DNS サーバから取得されたため、一時的です。セキュリティ アプライアンスは、72 時間の無活動後にこのエントリを削除します。 • perm：このエントリは **name** コマンドを使用して追加されたため、永続的です。 • OK：このエントリは有効です。 • ??：このエントリは疑わしいため、再検証が必要です。 • EX：このエントリは期限切れです。
Age	このエントリが最後に参照されてからの時間数を表示します。
Type	DNS レコードのタイプを表示します。この値は常に IP です。
Address(es)	IP アドレス。

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュをクリアします。
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。

show eigrp events

EIGRP イベント ログを表示するには、特権 EXEC モードで **show eigrp events** コマンドを使用します。

show eigrp [*as-number*] **events** [{*start end*} | **type**]

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
end	（任意）出力されるエントリを、インデックス番号 *start* で開始され、インデックス番号 *end* で終了するエントリに限定します。
start	（任意）ログ エントリのインデックス番号を指定する数値。開始番号を指定すると、出力は指定されたイベントで開始し、*end* 引数で指定されたイベントで終了します。有効な値は、1 ～ 4294967295 です。
type	（任意）記録されるイベントを表示します。

デフォルト

start および *end* を指定しない場合、すべてのログ エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show eigrp events の出力では最大 500 件のイベントが表示されます。イベントが最大数に到達すると、新しいイベントは出力の末尾に追加され、古いイベントは出力の先頭から削除されます。

clear eigrp events コマンドを使用すると、EIGRP イベント ログをクリアできます。

show eigrp events type コマンドは、EIGRP イベントのロギング ステータスを表示します。デフォルトでは、ネイバー変更、ネイバー警告、および DUAL FSM メッセージが記録されます。ネイバー変更イベントのロギングは、**no eigrp log-neighbor-changes** コマンドを使用してディセーブルにできます。ネイバー警告イベントのロギングは、**no eigrp log-neighbor-warnings** コマンドを使用してディセーブルにできます。DUAL FSM イベントのロギングはディセーブルにできません。

例

次に、**show eigrp events** コマンドの出力例を示します。

```
hostname# show eigrp events
```

```
Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

次に、**show eigrp events** コマンドで開始番号と終了番号を定義したときの出力例を示します。

```
hostname# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

次に、EIGRP イベント ログのエントリがない場合の **show eigrp events** コマンドの出力例を示します。

```
hostname# show eigrp events

Event information for AS 100:  Event log is empty.
```

次に、**show eigrp events type** コマンドの出力例を示します。

```
hostname# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

関連コマンド

コマンド	説明
clear eigrp events	EIGRP イベント ロギング バッファをクリアします。
eigrp log-neighbor-changes	ネイバー変更イベントのロギングをイネーブルにします。
eigrp log-neighbor-warnings	ネイバー警告イベントのロギングをイネーブルにします。

show eigrp interfaces

EIGRP ルーティングに参加しているインターフェイスを表示するには、特権 EXEC モードで **show eigrp interfaces** コマンドを使用します。

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

構文の説明

as-number	（任意）アクティブ インターフェイスを表示する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	（任意）詳細情報を表示します。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、指定されたインターフェイスに表示が制限されます。

デフォルト

インターフェイス名を指定しない場合、すべての EIGRP インターフェイスの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show eigrp interfaces コマンドを使用して、EIGRP がアクティブなインターフェイスを判別し、それらのインターフェイスに関連する EIGRP についての情報を学習します。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティング プロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

例

次に、**show eigrp interfaces** コマンドの出力例を示します。

```
hostname# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
```

```
mgmt          0         0/0           0       11/434           0           0
outside       1         0/0         337        0/10            0           0
inside        1         0/0          10        1/63          103           0
```

表 26-2 に、この出力で表示される重要なフィールドの説明を示します。

表 26-2　show eigrp interfaces のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Peers	直接接続されているピアの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均のスムーズ ラウンドトリップ時間間隔（秒）。
Pacing Time Un/Reliable	EIGRP パケット（信頼性の低いパケットおよび信頼性の高いパケット）をインターフェイスに送信するタイミングを決定するために使用されるペーシング時間（秒）。
Multicast Flow Timer	セキュリティ アプライアンスがマルチキャスト EIGRP パケットを送信する最大秒数。
Pending Routes	送信キュー内で送信を待機しているパケット内のルートの数。

関連コマンド

コマンド	説明
network	EIGRP ルーティング プロセスに参加するネットワークおよびインターフェイスを定義します。

show eigrp neighbors

EIGRP ネイバー テーブルを表示するには、特権 EXEC モードで **show eigrp neighbors** コマンドを使用します。

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	（任意）詳細なネイバー情報を表示します。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定する場合、そのインターフェイスを介して学習されたすべてのネイバー テーブル エントリが表示されます。
static	（任意）**neighbor** コマンドを使用してスタティックに定義された EIGRP ネイバーを表示します。

デフォルト

インターフェイス名を指定しない場合、すべてのインターフェイスを介して学習されたネイバーが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp neighbors コマンドを使用して、ダイナミックに学習されたネイバーを EIGRP ネイバー テーブルからクリアできます。

static キーワードを使用しない限り、スタティック ネイバーは出力に含まれません。

例

次に、**show eigrp neighbors** コマンドの出力例を示します。

```
hostname# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14       0:02:01  0      10   12    24
```

```
172.16.80.31            Ethernet0     12        0:02:02  0      4     5     20
```

表 26-3 に、この出力で表示される重要なフィールドの説明を示します。

表 26-3　show eigrp neighbors のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。
Holdtime	セキュリティ アプライアンスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、セキュリティ アプライアンスは、ネイバーを到達不能と見なします。
Uptime	セキュリティ アプライアンスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
Q Count	セキュリティ アプライアンスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、セキュリティ アプライアンスがそのパケットの確認応答を受信するために必要なミリ秒数です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、セキュリティ アプライアンスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。

次に、**show eigrp neighbors static** コマンドの出力例を示します。

```
hostname# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

表 26-4 に、この出力で表示される重要なフィールドの説明を示します。

表 26-4　show ip eigrp neighbors static のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Static Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。

次に、**show eigrp neighbors detail** コマンドの出力例を示します。

```
hostname# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

表 26-5 に、この出力で表示される重要なフィールドの説明を示します。

表 26-5　show ip eigrp neighbors details のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
H	このカラムは、指定されたネイバーとの間で確立されたピアリング セッションの順番を示します。順番は、0 から始まる連続した番号で指定されます。
Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。
Holdtime	セキュリティ アプライアンスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、セキュリティ アプライアンスは、ネイバーを到達不能と見なします。
Uptime	セキュリティ アプライアンスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、セキュリティ アプライアンスがそのパケットの確認応答を受信するために必要なミリ秒数です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、セキュリティ アプライアンスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。
Q Count	セキュリティ アプライアンスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
Version	指定されたピアが実行中のソフトウェア バージョン。
Retrans	パケットを再送した回数。

表 26-5　show ip eigrp neighbors details のフィールドの説明 （続き）

フィールド	説明
Retries	パケットの再送を試行した回数。
Restart time	指定されたネイバーが再起動してからの経過時間（時:分:秒）。

関連コマンド

コマンド	説明
clear eigrp neighbors	EIGRP ネイバー テーブルをクリアします。
debug eigrp neighbors	EIGRP ネイバー デバッグ メッセージを表示します。
debug ip eigrp	EIGRP パケット デバッグ メッセージを表示します。

show eigrp topology

EIGRP トポロジ テーブルを表示するには、特権 EXEC モードで **show eigrp topology** コマンドを使用します。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

構文の説明

active	（任意）EIGRP トポロジ テーブル内のアクティブ エントリのみ表示します。
all-links	（任意）EIGRP トポロジ テーブル内のすべてのルート（フィジブル サクセサでない場合も）を表示します。
as-number	（任意）EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
ip-addr	（任意）表示するトポロジ テーブルからの IP アドレス。マスクと一緒に指定した場合、エントリの詳細な説明が提供されます。
mask	（任意）*ip-addr* 引数に適用するネットワーク マスク。
pending	（任意）ネイバーからの更新を待機しているか、ネイバーへの応答を待機している、EIGRP トポロジ テーブル内のすべてのエントリを表示します。
summary	（任意）EIGRP トポロジ テーブルの要約を表示します。
zero-successors	（任意）EIGRP トポロジ テーブル内の使用可能なルートを表示します。

デフォルト

フィジブル サクセサであるルートのみが表示されます。**all-links** キーワードを使用すると、フィジブル サクセサでないものも含めたすべてのルートが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp topology コマンドを使用して、ダイナミック エントリをトポロジ テーブルから削除できます。

例

次に、**show eigrp topology** コマンドの出力例を示します。

```
hostname# show eigrp topology
```

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.16.90.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.16.81.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

表 26-6 に、この出力で表示される重要なフィールドの説明を示します。

表 26-6　show eigrp topology のフィールド情報

フィールド	説明
Codes	このトポロジ テーブル エントリの状態。Passive および Active は、この宛先に関する EIGRP 状態を示し、Update、Query、および Reply は、送信中のパケットのタイプを示します。
P - Passive	ルートは良好だと認識され、この宛先についての EIGRP 計算は実行されません。
A - Active	この宛先についての EIGRP 計算が実行されます。
U - Update	この宛先に更新パケットが送信されたことを示します。
Q - Query	この宛先にクエリー パケットが送信されたことを示します。
R - Reply	この宛先に応答パケットが送信されたことを示します。
r - Reply status	ソフトウェアがクエリーを送信し、応答を待機しているときに設定されるフラグ。
address mask	宛先の IP アドレスとマスク。
successors	サクセサの数。この数値は、IP ルーティング テーブル内のネクストホップの数に対応します。「successors」が大文字で表示される場合、ルートまたはネクスト ホップは遷移状態です。
FD	フィジブル ディスタンス。フィジブル ディスタンスは、宛先に到達するための最適なメトリックか、ルートがアクティブだったときに認識された最適なメトリックです。この値はフィジビリティ条件チェックに使用されます。レポートされたルータのディスタンス（スラッシュの後のメトリック）がフィジブル ディスタンスより小さい場合、フィジビリティ条件が満たされて、そのパスはフィジブル サクセサになります。ソフトウェアによってパスがフィジブル サクセサだと判断されると、その宛先にクエリーを送信する必要はありません。
via	この宛先についてソフトウェアに通知したピアの IP アドレス。これらのエントリの最初の *n* 個（*n* はサクセサの数）は、現在のサクセサです。リスト内の残りのエントリはフィジブル サクセサです。
(*cost*/*adv_cost*)	最初の数値は宛先へのコストを表す EIGRP メトリックです。2 番めの数値はこのピアがアドバタイズした EIGRP メトリックです。
interface	情報の学習元のインターフェイス。

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は内部ルートについてのものです。

```
hostname# show eigrp topology 10.2.1.0 255.255.255.0
```

```
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は外部ルートについてのものです。

```
hostname# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

関連コマンド

コマンド	説明
clear eigrp topology	ダイナミックに検出されたエントリを EIGRP トポロジ テーブルからクリアします。

show eigrp traffic

送受信された EIGRP パケットの数を表示するには、特権 EXEC モードで **show eigrp traffic** コマンドを使用します。

show eigrp [*as-number*] **traffic**

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp traffic コマンドを使用すると、EIGRP トラフィックの統計情報をクリアできます。

例

次に、**show eigrp traffic** コマンドの出力例を示します。

```
hostname# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

表 26-7 に、この出力で表示される重要なフィールドの説明を示します。

表 26-7　show eigrp traffic のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Hellos sent/received	送受信された hello パケットの数。
Updates sent/received	送受信された更新パケットの数。
Queries sent/received	送受信されたクエリー パケットの数。
Replies sent/received	送受信された応答パケットの数。
Acks sent/received	送受信された確認応答パケットの数。
Input queue high water mark/drops	最大受信しきい値に近づいている受信パケットの数と、ドロップされたパケットの数。
SIA-Queries sent/received	送受信されたアクティブ クエリーのスタック。
SIA-Replies sent/received	送受信されたアクティブ応答のスタック。

関連コマンド

コマンド	説明
debug eigrp packets	送受信された EIGRP パケットのデバッグ情報を表示します。
debug eigrp transmit	送信された EIGRP メッセージのデバッグ情報を表示します。

show failover

ユニットのフェールオーバー ステータスに関する情報を表示するには、特権 EXEC モードで **show failover** コマンドを使用します。

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

構文の説明

group	指定されたフェールオーバー グループの実行状態を表示します。
history	フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。履歴情報はデバイスをリブートするとクリアされます。
interface	フェールオーバー コマンドとステートフル リンクの情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー ユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。障害の理由が解消されても、障害の理由は出力に残ります。
statistics	フェールオーバー コマンド インターフェイスの送信および受信パケット数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。出力の情報が追加されました。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバー情報、インターフェイス ステータス、およびステートフル フェールオーバーの統計情報を表示します。Stateful Failover Logical Update Statistics 出力は、ステートフル フェールオーバーがイネーブルの場合のみ表示されます。「xerr」および「rerr」の値はフェールオーバーのエラーではなく、パケット送受信エラーの数を示します。

（注） ステートフル フェールオーバーは、ASA 5505 セキュリティ アプライアンスでは使用できません。したがって、ステートフル フェールオーバーの統計情報出力も使用できません。

show failover コマンド出力で、ステートフル フェールオーバーの各フィールドには次の値があります。

- Stateful Obj の値は次のとおりです。
  - xmit：送信されたパケットの数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケットの数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定のオブジェクト スタティック カウントを表します。
  - General：すべてのステートフル オブジェクトの合計を示します。
  - sys cmd：**login** または **stay alive** などの論理的なシステム更新コマンドを示します。
  - up time：セキュリティ アプライアンスのアップ タイムの値（アクティブなセキュリティ アプライアンスがスタンバイのセキュリティ アプライアンスに渡す）を示します。
  - RPC services：リモート プロシージャ コール接続情報。
  - TCP conn：ダイナミック TCP 接続情報。
  - UDP conn：ダイナミック UDP 接続情報。
  - ARP tbl：ダイナミック ARP テーブル情報。
  - Xlate_Timeout：接続変換タイムアウト情報を示します。
  - VPN IKE upd：IKE 接続情報。
  - VPN IPSEC upd：IPSec 接続情報。
  - VPN CTCP upd：cTCP トンネル接続情報。
  - VPN SDI upd：SDI AAA 接続情報。
  - VPN DHCP upd：トンネル型 DHCP 接続情報。
  - SIP Sesson：SIP シグナリング セッション情報。

フェールオーバー IP アドレスを入力しない場合、**show failover** コマンドでは IP アドレス 0.0.0.0 が表示され、インターフェイスのモニタリングは「waiting」状態のままになります。フェールオーバーを機能させるにはフェールオーバー IP アドレスを設定する必要があります。

表 26-8 に、フェールオーバーのインターフェイス状態の説明を示します。

表 26-8　フェールオーバー インターフェイス状態

状態	説明
Normal	インターフェイスは稼働中で、ピア ユニットの対応するインターフェイスから hello パケットを受信中です。
Normal (Waiting)	インターフェイスは稼働中ですが、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
Normal (Not-Monitored)	インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
No Link	物理リンクがダウンしています。

表 26-8　フェールオーバー インターフェイス状態 （続き）

状態	説明
No Link (Waiting)	物理リンクがダウンし、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。リンクが復元した後、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
No Link (Not-Monitored)	物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Link Down	物理リンクは動作中ですが、インターフェイスは管理上ダウンしています。
Link Down (Waiting)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスを動作状態にした後（インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを使用）、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
Link Down (Not-Monitored)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Testing	ピア ユニットの対応するインターフェイスから hello パケットが届かないため、インターフェイスはテスト モードです。
Failed	インターフェイスのテストに失敗し、インターフェイスは障害が発生したとしてマークされます。インターフェイスの障害によってフェールオーバー基準が満たされた場合、インターフェイスの障害によって、セカンダリ ユニットまたはフェールオーバー グループへのフェールオーバーが発生します。

マルチ コンフィギュレーション モードでは、**show failover** コマンドのみがセキュリティ コンテキストで使用でき、任意のキーワードを入力できません。

例

次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。セキュリティ アプライアンスは ASA 5500 シリーズのセキュリティ アプライアンスで、各セキュリティ アプライアンスのスロット 1 に詳細を示すように、それぞれ CSC SSM を装備しています。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
```

```
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3): Normal
                  Interface outside (10.132.9.3): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4): Normal
                  Interface outside (10.132.9.4): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

次に、Active/Active フェールオーバーでの **show failover** コマンドの出力例を示します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
```

```
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
       SIP Session    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

次に、ASA 5505 シリーズのセキュリティ アプライアンスでの **show failover** コマンドの出力例を示します。

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
```

```
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

次に、アクティブ-アクティブ セットアップでの **show failover state** コマンドの出力例を示します。

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

次に、アクティブ-スタンバイ セットアップでの **show failover state** コマンドの出力例を示します。

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 26-9 に、**show failover state** コマンドの出力の説明を示します。

表 26-9　show failover state の出力の説明

フィールド	説明
Configuration State	コンフィギュレーションの同期化の状態を表示します。 スタンバイ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing - STANDBY**：コンフィギュレーションの同期化が実行されているときに設定されます。 • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**：スタンバイ ユニットが、アクティブ ユニットとのコンフィギュレーションの同期化を完了したときに設定されます。 アクティブ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing**：スタンバイ ユニットに対してコンフィギュレーションの同期化を実行しているときにアクティブ ユニット上で設定されます。 • **Interface Config Syncing** • **Sync Done**：アクティブ ユニットが、スタンバイ ユニットに対してコンフィギュレーションの同期化を正常に完了したときに設定されます。 • **Ready for Config Sync**：スタンバイ ユニットがコンフィギュレーションの同期化を受信する準備が完了したという信号を送るときにアクティブ ユニット上で設定されます。
Communication State	MAC アドレスの同期化のステータスを表示します。 • **Mac set**：MAC アドレスがピア ユニットからこのユニットに同期化されました。 • **Updated Mac**：MAC アドレスが更新され、他のユニットに対して同期化する必要がある場合に使用されます。また、ユニットが遷移期間中に、ピア ユニットから同期化されたローカル MAC アドレスを更新する場合にも使用されます。
Date/Time	障害の日付およびタイムスタンプを表示します。
Last Failure Reason	最後にレポートされた障害の理由を表示します。この情報は、障害の条件が解消されてもクリアされません。この情報は、フェールオーバーが発生した場合にのみ変更されます。 可能な障害の理由は次のとおりです。 • **Ifc Failure**：障害が発生したインターフェイスの数がフェールオーバー基準を満たし、フェールオーバーが発生しました。 • **Comm Failure**：フェールオーバー リンクに障害が発生したか、ピアがダウンしています。 • **Backplane Failure**

表 26-9　show failover state の出力の説明 （続き）

フィールド	説明
State	ユニットの Primary/Secondary および Active/Standby ステータスを表示します。
This host/Other host	This host は、コマンドが実行されたデバイスについての情報を示します。Other host は、フェールオーバーのペアとなる他のデバイスについての情報を示します。

次に、**show failover history** コマンドの出力例を示します。

```
hostname# show failover history

==========================================================================
From State                To State                  Reason
==========================================================================
At   16:28:50 UTC Sep 9 2006
Not Detected              Negotiation               No Error

At   16:29:18 UTC Sep 9 2006
Negotiation               Cold Standby              Detected an Active mate

At   16:29:19 UTC Sep 9 2006
Cold Standby              Sync Config               Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync Config               Sync File System          Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync File System          Bulk Sync                 Detected an Active mate

At   16:29:36 UTC Sep 9 2006
Bulk Sync                 Standby Ready             Detected an Active mate

At   16:30:52 UTC Sep 9 2006
Standby Ready             Just Active               Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Just Active               Active Drain              Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Drain              Active Applying Config    Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Applying Config    Active Config Applied     Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Config Applied     Active                    Set by the CI config cmd

At   16:30:55 UTC Sep 9 2006
Active                    Disabled                  Set by the CI config cmd

==========================================================================
```

各エントリには、状態変更が発生した時刻および日付、開始状態、結果状態、および状態変更の理由が示されます。最も新しいエントリが表示の末尾に配置されます。古いエントリが上部に表示されます。最大で 60 エントリを表示できます。エントリが最大数に到達した場合、最も古いエントリが出力の上部から削除され、新しいエントリが末尾に追加されます。

表 26-10 に、フェールオーバーの状態を示します。状態には永続的と一時的の 2 つのタイプがあります。永続的な状態とは、障害などの何らかの出来事によって状態変更が発生するまで、ユニットが維持できる状態のことです。一時的な状態とは、ユニットが永続的な状態に到達するまでの間に経過する状態です。

表 26-10　フェールオーバーの状態

State	説明
Initialization	装置はプラットフォームの機能およびコンフィギュレーションをチェックし、フェールオーバー通信チャネルを準備しています。これは一時的なステートです。
Disabled	フェールオーバーはディセーブルです。これは安定したステートです。
Negotiation	ユニットはピアとの接続を確立し、ピアとネゴシエートして、ソフトウェア バージョンの互換性を判別し、Active/Standby ロールを決定します。ネゴシエートされたロールに基づき、ユニットはスタンバイ ユニット状態またはアクティブ ユニット状態になるか、障害状態になります。これは一時的なステートです。
Failed	ユニットは障害状態です。これは安定したステートです。
スタンバイ ユニット状態	
Cold Standby	ユニットはピアがアクティブ状態に到達するのを待機します。ピア ユニットがアクティブ状態に到達すると、このユニットは Standby Config 状態に進みます。これは一時的なステートです。
Sync Config	ユニットはピア ユニットから実行コンフィギュレーションを要求します。コンフィギュレーションの同期化中にエラーが発生した場合、ユニットは初期化状態に戻ります。これは一時的なステートです。
Sync File System	ユニットはピア システムとファイル システムを同期化します。これは一時的なステートです。
Bulk Sync	ユニットはピアから状態情報を受信します。この状態は、ステートフル フェールオーバーがイネーブルの場合にのみ発生します。これは一時的なステートです。
Standby Ready	ユニットは、アクティブ ユニットに障害が発生した場合に引き継ぐ準備が完了しています。これは安定したステートです。
アクティブ ユニット状態	
Just Active	ユニットがアクティブ ユニットになったときの最初の状態です。この状態にあるとき、ユニットがアクティブになること、および IP アドレスと MAC アドレスをインターフェイスに設定することをピアに通知するメッセージがピアに送信されます。これは一時的なステートです。
Active Drain	ピアからのキュー メッセージが廃棄されます。これは一時的なステートです。
Active Applying Config	ユニットはシステム コンフィギュレーションを適用します。これは一時的なステートです。
Active Config Applied	ユニットはシステム コンフィギュレーションの適用を完了しました。これは一時的なステートです。
Active	ユニットはアクティブで、トラフィックを処理しています。これは安定したステートです。

それぞれの状態変更の後に状態変更の理由が続きます。この理由は、ユニットが一時的な状態から永続的な状態に進んでも、通常同じままになります。次に、可能性がある状態変更の理由を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他のユニットのソフトウェア バージョンが異なっている
- 他のユニットの動作モードが異なっている
- 他のユニットのライセンスが異なっている
- 他のユニットのシャーシ コンフィギュレーションが異なっている
- 他のユニットのカード コンフィギュレーションが異なっている
- 他のユニットからアクティブ状態を要求された
- 他のユニットからスタンバイ状態を要求された
- 他のユニットが、このユニットに障害があるとレポートした
- 他のユニットが、そのユニットに障害があるとレポートした
- コンフィギュレーションの不一致
- アクティブ ユニットが検出された
- アクティブ ユニットが検出されなかった
- コンフィギュレーションの同期化が行われた
- 通信障害から回復した
- 他のユニットの VLAN コンフィギュレーションが異なっている
- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- このユニットの通信が失敗した
- フェールオーバー メッセージの ACK を受信しなかった
- 同期後の学習状態で他のユニットが動作しなくなった
- ピアの電源が検出されない
- フェールオーバー ケーブルがない
- HA 状態の進行に失敗した
- サービス カード障害が検出された
- 他のユニットのサービス カードに障害が発生した
- このユニットのサービス カードはピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア ユニットがリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーション同期化の状態を確認できない
- 自動更新要求

- 原因不明

関連コマンド

コマンド	説明
show running-config failover	現在のコンフィギュレーション内の **failover** コマンドを表示します。

show failover exec

指定したユニットの **failover exec** コマンド モードを表示するには、特権 EXEC モードで **show failover exec** コマンドを使用します。

show failover exec {**active** | **standby** | **mate**}

構文の説明

active	アクティブ ユニットの **failover exec** コマンド モードを表示します。
mate	ピア ユニットの **failover exec** コマンド モードを表示します。
standby	スタンバイ ユニットの **failover exec** コマンド モードを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

failover exec コマンドは、指定したデバイスとのセッションを確立します。デフォルトでは、このセッションはグローバル コンフィギュレーション モードです。このセッションのコマンド モードは、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信することによって変更できます。指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。

show failover exec コマンドは、**failover exec** コマンドで送信されるコマンドが実行される、指定したデバイス上のコマンド モードを表示します。

例

次に、**show failover exec** コマンドの出力例を示します。この例では、**failover exec** コマンドが入力されるユニットのコマンド モードが、コマンドが実行される **failover exec** コマンド モードと同じである必要がないことを示しています。

この例では、スタンバイ ユニットにログインした管理者が、アクティブ ユニット上のインターフェイスに名前を追加します。この例で、**show failover exec mate** コマンドを 2 回めに入力したとき、ピア デバイスはインターフェイス コンフィギュレーション モードであると表示されます。**failover exec** コマンドでデバイスに送信されるコマンドは、このモードで実行されます。

```
hostname(config)# show failover exec mate
```

```
Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
hostname(config)# failover exec mate interface GigabitEthernet0/1
hostname(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
hostname(config)# failover exec mate nameif test
```

関連コマンド

コマンド	説明
failover exec	フェールオーバー ペアの指定されたユニット上で、入力されたコマンドを実行します。

show file

ファイル システムについての情報を表示するには、特権 EXEC モードで **show file** コマンドを使用します。

show file descriptors | system | information *filename*

構文の説明

descriptors	開かれているファイル記述子をすべて表示します。
information	特定のファイルに関する情報を表示します。
filename	ファイル名を指定します。
system	ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ファイル システム情報を表示する例を示します。

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
pwd	現在の作業ディレクトリを表示します。

show firewall

現在のファイアウォール モード（ルーテッドまたはトランスペアレント）を表示するには、特権 EXEC モードで **show firewall** コマンドを使用します。

show firewall

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show firewall** コマンドの出力例を示します。

```
hostname# show firewall
Firewall mode: Router
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを設定します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

show flash

内部フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show flash:** コマンドを使用します。

show flash:

（注）　ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例は、内部フラッシュ メモリの内容を表示する方法を示しています。

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
```

```
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show disk0	内部フラッシュ メモリの内容を表示します。
show disk1	外部フラッシュ メモリ カードの内容を表示します。

show fragment

IP フラグメント再構築モジュールの動作データを表示するには、特権 EXEC モードで **show fragment** コマンドを使用します。

show fragment [*interface*]

構文の説明

interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データと動作データを分けるために、**show fragment** および **show running-config fragment** の 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データを表示する方法の例を示します。

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。

コマンド	説明
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show gc

ガーベッジ コレクション プロセスの統計情報を表示するには、特権 EXEC モードで **show gc** コマンドを使用します。

show gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show gc** コマンドの出力例を示します。

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :           0
Total udp conn delete response             :           0
Total number of zombie cleaned             :           0
Total number of embryonic conn cleaned     :           0
Total error response                       :           0
Total queries generated                    :           0
Total queries with conn present response   :           0
Total number of sweeps                     :         946
Total number of invalid vcid               :           0
Total number of zombie vcid                :           0
```

関連コマンド

コマンド	説明
clear gc	ガーベッジ コレクション プロセスの統計情報を削除します。

show h225

セキュリティ アプライアンスを越えて確立された H.225 セッションの情報を表示するには、特権 EXEC モードで **show h225** コマンドを使用します。

show h225

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show h225 コマンドは、セキュリティ アプライアンス を越えて確立されている H.225 セッションの情報を表示します。このコマンドは、**debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドとともに、H.323 インスペクション エンジンの問題のトラブルシューティングに使用されます。

show h225、**show h245**、または **show h323-ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。セッション レコードが多いときに **pager** コマンドが設定されていない場合、**show** コマンドの出力が末端に届くまでに時間がかかる場合があります。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

例

次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
|Local:|10.130.56.3/1040|Foreign: 172.30.254.203/1720
|1. CRV 9861
|Local:|10.130.56.3/1040|Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
|Local:|10.130.56.4/1050|Foreign: 172.30.254.205/1720
```

この出力は、ローカル エンドポイント 10.130.56.3 と外部ホスト 172.30.254.203 との間でセキュリティ アプライアンスを通過するアクティブな H.323 コールが 1 つ存在し、これらのエンドポイントの間には、コールの CRV（Call Reference Value）が 9861 の同時コールが 1 つ存在することを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 については、同時コールの数は 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h245

スロー スタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示するには、特権 EXEC モードで **show h245** コマンドを使用します。

show h245

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show h245 コマンドは、スロースタートを使用しているエンドポイントが セキュリティ アプライアンス を越えて確立した H.245 セッションの情報を表示します。（スロー スタートでは、コールの 2 つのエンドポイントが H.245 用に別の TCP コントロール チャネルを開きます。ファースト スタートは、H.245 メッセージが H.225 コントロール チャネル上の H.225 メッセージの一部として交換された場合です。このコマンドは、**debug h323 h245 event**、**debug h323 h225 event**、および **show local-host** コマンドとともに、H.323 インスペクション エンジンの問題のトラブルシューティングに使用されます。

例

次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
| LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
| MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
| Local | 10.130.56.3 RTP 49608 RTCP 49609
| MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
| Local | 10.130.56.3 RTP 49606 RTCP 49607
```

セキュリティ アプライアンスでアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。（TKTP ヘッダーは、各 H.225/H.245 メッセージの先頭の 4 バイト ヘッダーです。このヘッダーは、4 バイト ヘッダーを含むメッセージの長さを指定します）。外部ホスト エンドポイントは 172.30.254.203 で、TPKT 値が 0 のため、このエンドポイントからの次のパケットが TPKT ヘッダーを持つことが予想されます。

これらのエンドポイント間でネゴシエートされるメディアは、Logical Channel Number（LCN; 論理チャネル番号）が 258 で、外部の RTP IP アドレス / ポート ペアが 172.30.254.203/49608、RTCP IP アドレス / ポートが 172.30.254.203/49609、ローカルの RTP IP アドレス / ポート ペアが 10.130.56.3/49608、RTCP ポートが 49609 です。

値が 259 の 2 番めの LCN は、外部の RTP IP アドレス / ポート ペアが 172.30.254.203/49606、RTCP IP アドレス / ポート ペアが 172.30.254.203/49607、ローカルの RTP IP アドレス / ポート ペアが 10.130.56.3/49606、RTCP ポートが 49607 です。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h323-ras

ゲートキーパーとその H.323 エンドポイントの間でセキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示するには、特権 EXEC モードで **show h323-ras** コマンドを使用します。

show h323-ras

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show h323-ras コマンドは、セキュリティ アプライアンス を越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。このコマンドは、**debug h323 ras event** および **show local-host** コマンドとともに、H.323 RAS インスペクション エンジンの問題のトラブルシューティングに使用されます。

show h323-ras コマンドは、H.323 インスペクション エンジンの問題をトラブルシューティングするための接続情報を表示し、**inspect protocol h323 {h225 | ras}** コマンド ページに説明されています。

例

次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
|GK|Caller
|172.30.254.214 10.130.56.14
hostname#
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show history

以前入力したコマンドを表示するには、ユーザ EXEC モードで **show history** コマンドを使用します。

show history

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show history コマンドを使用すると、以前入力したコマンドを表示できます。上矢印と下矢印を使用してコマンドを個別に調べて、**^p** を入力して以前に入力した行を表示するか、**^n** を入力して次の行を表示できます。

例

次の例は、以前に入力したコマンドをユーザ EXEC モードに入っているときに表示する方法を示しています。

```
hostname> show history
    show history
    help
    show history
```

次の例は、以前に入力したコマンドを特権 EXEC モードに入っているときに表示する方法を示しています。

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

次の例は、以前に入力したコマンドをグローバル コンフィギュレーション モードに入っているときに表示する方法を示しています。

```
hostname(config)# show history
    show history
```

```
help
show history
enable
show history
config t
show history
```

関連コマンド

コマンド	説明
help	指定したコマンドのヘルプ情報を表示します。

show icmp

ICMP コンフィギュレーションを表示するには、特権 EXEC モードで **show icmp** コマンドを使用します。

show icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show icmp コマンドは ICMP コンフィギュレーションを表示します。

例

次に、ICMP コンフィギュレーションを表示する例を示します。

```
hostname# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

Interface Descriptor Block のステータスについての情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

show idb

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IDB はインターフェイス リソースを表す内部データ構造です。出力表示の詳細については、「例」を参照してください。

例

次に、**show idb** コマンドの出力例を示します。

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
              Active 6          21
            Inactive 1          2
          Total IDBs 7          23
 Size each (bytes) 116        212
        Total bytes 812        4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
```

```
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

表 26-11 に、各フィールドの説明を示します。

表 26-11　show idb stats の各フィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システム内の各ハードウェア ポートについて作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システム内の各メインおよびサブインターフェイスについて、およびコンテキストに割り当てられている各インターフェイスについて作成されます。 他の一部の内部ソフトウェア モジュールも IDB を作成します。
HWIDB#	ハードウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show igmp groups

セキュリティ アプライアンスに直接接続された受信者、および IGMP によって学習された受信者を含むマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

構文の説明

detail	（任意）ソースの詳細説明を出力します。
group	（任意）IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。
if_name	（任意）指定されたインターフェイスについてのグループ情報を表示します。
reserved	（任意）予約されたグループについての情報を表示します。
summary	（任意）グループ加入の要約情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたマルチキャスト グループを、グループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

次に、**show igmp groups** コマンドの出力例を示します。

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

show igmp interface

インターフェイスのマルチキャスト情報を表示するには、特権 EXEC モードで **show igmp interface** コマンドを使用します。

show igmp interface [*if_name*]

構文の説明

if_name	（任意）選択したインターフェイスについての IGMP グループ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。**detail** キーワードが削除されました。

使用上のガイドライン

オプションの *if_name* 引数を省略すると、**show igmp interface** コマンドはすべてのインターフェイスについての情報を表示します。

例

次に、**show igmp interface** コマンドの出力例を示します。

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。

show igmp traffic

IGMP トラフィックの統計情報を表示するには、特権 EXEC モードで **show igmp traffic** コマンドを使用します。

show igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show igmp traffic** コマンドの出力例を示します。

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP 統計カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

show import webvpn

セキュリティ アプライアンスのフラッシュ メモリに現在存在する WebVPN カスタム データとプラグインをリストするには、特権 EXEC モードで **show import webvpn**（*任意*）コマンドを入力します。

show import webvpn | customization | plug-in | plug-in detail | translation-table | url-list | webcontent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show import webvpn コマンドを使用すると、WebVPN ユーザが使用可能なカスタム データおよび Java ベースのクライアント アプリケーションが識別されます。表示されるリストでは、セキュリティ アプライアンスのフラッシュ メモリにある要求されるすべてのデータ タイプの詳細が表示されます。

それぞれの show import webvpn コマンドでは、次に示す現在ロードされている WebVPN データが表示されます。

- カスタマイゼーション：カスタマイゼーション オブジェクト（ファイル名は base64 でデコード）
- プラグイン：サード パーティ製 Java ベースのクライアント アプリケーション（SSH、VNC、および RDP）
- プラグインの詳細情報：各プラグインのハッシュ情報と日付情報
- 変換テーブル：ローカリゼーションおよび国際化辞書テーブル
- URL リスト：URL リスト オブジェクト（ファイル名は base64 でデコード）
- Web コンテンツ：再帰的な disk0:/csco_config/htms（すべてのファイルのフルネーム）

例

次に、さまざまな **show import webvpn** コマンドによって表示される WebVPN データの例を示します。

```
hostname# show import webvpn plug-in
ssh
rdp
```

```
vnc
hostname#

hostname# show import webvpn customization
Template
DfltCustomization
hostname#

hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
hostname#

hostname# show import webvpn url-list
Template
No bookmarks are currently defined
hostname#

hostname# show import webvpn webcontent
No custom webcontent is loaded
hostname#
```

関連コマンド

コマンド	説明
revert webvpn all	セキュリティ アプライアンスに現在存在するすべての WebVPN データおよびプラグインを削除します。

show interface

インターフェイス統計情報を表示するには、特権 EXEC モードで **show interface** コマンドを使用します。

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [**stats** | **detail**]

構文の説明

detail	（任意）インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態、非対称ルーティングの統計情報（**asr-group** コマンドによって非対称ルーティングがイネーブルになっている場合）が含まれます。すべてのインターフェイスを表示する場合、SSM 用の内部インターフェイスが ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールされているとき、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabitethernet 0/1** のようなインターフェイス ID を識別します。有効値については、**interface** コマンドを参照してください。
redundant*number*	（任意）**redundant1** のような冗長インターフェイス ID を識別します。
stats	（デフォルト）インターフェイス情報および統計情報を表示します。このキーワードはデフォルトであるため、このキーワードはオプションです。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

いずれのオプションも識別しない場合、このコマンドはすべてのインターフェイスについての基本的な統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいインターフェイス番号付け方式を取り入れるように変更され、明示的に指定するための **stats** キーワード、および **detail** キーワードが追加されました。
7.0(4)	このコマンドに、4GE SSM インターフェイス用のサポートが追加されました。
7.2(1)	このコマンドに、スイッチ インターフェイス用のサポートが追加されました。
8.0(2)	このコマンドに、冗長インターフェイス用のサポートが追加されました。また、サブインターフェイス用の遅延が追加されました。入力リセット ドロップと出力リセット ドロップの 2 つの新しいカウンタが追加されました。

使用上のガイドライン

1 つのインターフェイスが複数のコンテキストで共有されているときに、あるコンテキストでこのコマンドを入力した場合、セキュリティ アプライアンスは現在のコンテキストの統計情報だけを表示します。物理インターフェイスのシステム実行スペース内でこのコマンドを使用すると、セキュリティ アプライアンスはすべてのコンテキストについて組み合わせた統計情報を表示します。

サブインターフェイスについて表示される統計情報の数は、物理インターフェイスについて表示される統計情報の数のサブセットです。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。**allocate-interface** コマンドで **visible** キーワードを設定した場合、セキュリティ アプライアンスは **show interface** コマンドの出力にインターフェイス ID を表示します。

（注） Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

ハードウェア カウントでは、トラフィック量はハードウェアから直接取得され、レイヤ 2 のパケットサイズが反映されます。一方、Traffic Statistics では、レイヤ 3 パケットのサイズが反映されます。

カウントの差はインターフェイス カード ハードウェアの設計に基づいて異なります。

たとえば、ファスト イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーを含むため、トラフィック カウントよりも 14 バイト大きくなります。ギガビット イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーと CRC の両方を含むため、トラフィック カウントよりも 18 バイト大きくなります。

出力表示の詳細については、「例」を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
hostname# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
```

```
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
```

```
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
```

```
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

表 26-12 に、各フィールドの説明を示します。

表 26-12　show interface のフィールド

フィールド	説明
Interface *ID*	インターフェイス ID。コンテキスト内では、**allocate-interface** コマンドで **visible** キーワードを設定しない限り、セキュリティ アプライアンスはマッピング名（設定されている場合）を表示します。
"*interface_name*"	**nameif** コマンドで設定されたインターフェイス名。システム実行スペースでは、システムに名前を設定できないため、このフィールドはブランクです。名前を設定しない場合、Hardware 行の下に次のメッセージが表示されます。 `Available but not configured via nameif`
is *state*	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Line protocol is *state*	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。
VLAN identifier	サブインターフェイスの場合、VLAN ID。
Hardware	インターフェイスのタイプ、最大帯域幅、遅延、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコで囲まれて設定値とともに表示されます。次に、一般的なハードウェア タイプを示します。 • i82542：PIX プラットフォームで使用される Intel PCI ファイバ ギガビット カード • i82543：PIX プラットフォームで使用される Intel PCI-X ファイバ ギガビット カード • i82546GB：ASA プラットフォーム上で使用される Intel PCI-X 銅線ギガビット • i82547GI：ASA プラットフォーム上でバックプレーンとして使用される Intel CSA 銅線ギガビット • i82557：ASA プラットフォーム上で使用される Intel PCI 銅線ファスト イーサネット • i82559：PIX プラットフォームで使用される Intel PCI 銅線ファスト イーサネット • VCS7380：SSM-4GE で使用される Vitesse 4 ポート ギガビット スイッチ

表 26-12　show interface のフィールド （続き）

フィールド	説明
Media-type	（4GE SSM インターフェイスの場合のみ）インターフェイスが RJ-45 または SFP のいずれとして設定されているかを示します。

message area	一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。
	• システム実行スペースで、次のメッセージが表示される場合があります。
	`Available for allocation to a context`
	• 名前を設定しない場合、次のメッセージが表示されます。
	`Available but not configured via nameif`
	• インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。
	`Active member of Redundant5`

MAC address	インターフェイスの MAC アドレス。
MTU	このインターフェイス上で許可されるパケットの最大サイズ（バイト単位）。インターフェイス名を設定しない場合、このフィールドには「MTU not set」と表示されます。
IP address	**ip address** コマンドを使用して設定したか、DHCP サーバから受信したインターフェイスの IP アドレス。システム実行スペースでは、システムに IP アドレスを設定できないため、このフィールドには「IP address unassigned」と表示されます。
Subnet mask	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信したパケットの数。
Bytes	このインターフェイスで受信したバイト数。
No buffer	メイン システムのバッファ スペースがなかったために、廃棄された受信済みパケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
Received:	
Broadcasts	受信したブロードキャストの数。
Input errors	次に示すタイプを含めた入力エラーの総数。入力に関係する他のエラーも入力エラーのカウントが増加する原因になります。また、一部のデータグラムは複数のエラーを含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。
Runts	最小のパケット サイズ（64 バイト）よりも小さいために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。
Giants	最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

表 26-12　show interface のフィールド （続き）

フィールド	説明
CRC	Cyclical Redundancy Check（CRC; 巡回冗長検査）エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、セキュリティ アプライアンスは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。
Frame	フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。
Overrun	セキュリティ アプライアンスのデータ処理能力を入力レートが超えたため、セキュリティ アプライアンスがハードウェア バッファに受信したデータを処理できなかった回数。
Ignored	このフィールドは使用されません。値は常に 0 です。
Abort	このフィールドは使用されません。値は常に 0 です。
L2 decode drops	名前がまだ設定されていないか（**nameif** コマンド）、無効な VLAN ID を持つフレームが受信されたためにドロップしたパケットの数。
Packets output	このインターフェイスに送信されたパケットの数。
Bytes	このインターフェイスに送信されたバイトの数。
Underruns	セキュリティ アプライアンスが処理できるよりも速くトランスミッタが稼働した回数。
Output Errors	設定されたコリジョンの最大数を超えたため送信されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。
Collisions	イーサネット コリジョン（単一および複数のコリジョン）が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスで 3 秒間送信できない場合、セキュリティ アプライアンスはインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。インターフェイスのリセットは、インターフェイスがループバックまたはシャットダウンする場合も発生します。
Babbles	未使用。（「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します）。

表 26-12　show interface のフィールド （続き）

フィールド	説明
Late collisions	通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。 レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、セキュリティ アプライアンスはパケットの送信を部分的に完了しています。セキュリティ アプライアンスは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で送信前に保留されたフレームの数。
input reset drops	リセットが発生したときに RX リングでドロップしたパケットの数をカウントします。
output reset drops	リセットが発生したときに TX リングでドロップしたパケットの数をカウントします。
Rate limit drops	（4GE SSM インターフェイスの場合だけ）ギガビット以外の速度でインターフェイスを設定して、設定に応じて 10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。
Lost carrier	送信中に搬送波信号が消失した回数。
No carrier	未使用。
Input queue (curr/max packets):	入力キュー内のパケットの数（現行値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。ギガビット イーサネット インターフェイスでは使用できません。
Output queue (curr/max packets):	出力キュー内のパケットの数（現行値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Traffic Statistics:	受信、送信、またはドロップしたパケットの数。
Packets input	受信したパケットの数とバイトの数。
Packets output	送信したパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。このカウンタは通常、Accelerated Security Path（ASP; 高速セキュリティ パス）上でドロップしたパケットについて増分します（たとえば、アクセス リスト拒否が原因でパケットをドロップした場合など）。 インターフェイス上でドロップが発生する原因については、**show asp drop** コマンドを参照してください。

表 26-12　show interface のフィールド （続き）

フィールド	説明
1 minute input rate	過去 1 分間に受信したパケットの数（パケット / 秒およびバイト / 秒）。
1 minute output rate	過去 1 分間に送信したパケットの数（パケット / 秒およびバイト / 秒）。
1 minute drop rate	過去 1 分間にドロップしたパケットの数（パケット / 秒）。
5 minute input rate	過去 5 分間に受信したパケットの数（パケット / 秒およびバイト / 秒）。
5 minute output rate	過去 5 分間に送信したパケットの数（パケット / 秒およびバイト / 秒）。
5 minute drop rate	過去 5 分間にドロップしたパケットの数（パケット / 秒）。
Redundancy Information:	冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブ インターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。 メンバーをまだ割り当てていない場合、次の出力が表示されます。 `Members unassigned`
Last switchover	冗長インターフェイスの場合、アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした時刻を表示します。

次に、スイッチ ポートを含む ASA 5505 適応型セキュリティ アプライアンス上での **show interface** コマンドの出力例を示します。

```
hostname# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

表 26-13 に、ASA 5505 適応型セキュリティ アプライアンスのスイッチ インターフェイスなどのスイッチ インターフェイスに対する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 26-1 を参照してください。

表 26-13　スイッチ インターフェイスの show interface のフィールド

フィールド	説明
switch ingress policy drops	このドロップは通常、ポートが正しく設定されていないときに表示されます。このドロップは、デフォルトまたはユーザ設定のスイッチ ポート設定の結果としてスイッチ ポート内でパケットが正常に転送できない場合に増分されます。このドロップの原因として、次のコンフィギュレーションが考えられます。 • **nameif** コマンドが VLAN インターフェイス上で設定されていない。 **（注）** 同じ VLAN 内のインターフェイスに、**nameif** コマンドが設定されていなかった場合でも、VLAN 内のスイッチングは正常で、このカウンタは増分されません。 • VLAN がシャットダウンしている。 • アクセス ポートで 802.1Q タグが付いたパケットを受信した。 • トランク ポートで許可されないタグまたはタグのないパケットを受信した。 • セキュリティ アプライアンスが、イーサネット キープアライブを持つ別のシスコ デバイスに接続されている。たとえば、Cisco IOS ソフトウェアではインターフェイス ヘルス状態を確認するためにイーサネット ループバック パケットを使用します。このパケットは、他のデバイスによって受信されるためのものではなく、パケットをただ送信できることによって、ヘルス状態が確認されます。これらのタイプのパケットはスイッチ ポートでドロップされ、カウンタが増分されます。 • VLAN に物理インターフェイスが 1 つしか存在しないが、パケットの DEST は VLAN の MAC アドレスと一致せず、ブロードキャスト アドレスでない。
switch egress policy drops	現在使用されていません。

次に、**show interface detail** コマンドの出力例を示します。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（**asr-group** コマンドでイネーブルにされている場合）を表示する例を示します。

```
hostname# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
```

```
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 26-14 に、**show interface detail** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 26-1 を参照してください。

表 26-14　show interface detail の各フィールド

フィールド	説明
Demux drops	（内部データ インターフェイスのみ）セキュリティ アプライアンスが SSM インターフェイスからのパケットを逆多重化できなかったためドロップしたパケットの数。SSM インターフェイスはバックプレーンを介してネイティブ インターフェイスと通信し、すべての SSM インターフェイスからのパケットはバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	デバッグに使用される 0 から始まる番号で、このインターフェイスが作成された順番を示します。
Interface config status	管理ステートは次のとおりです。 • active：インターフェイスはシャット ダウンされていません。 • not active：インターフェイスは **shutdown** コマンドでシャット ダウンされています。
Interface state	インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。ハイ アベイラビリティに設定した場合、セキュリティ アプライアンスは必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信した ASR パケットの数。

表 26-14　show interface detail の各フィールド （続き）

フィールド	説明
Transmitted X2 packets	このインターフェイスで送信した ASR パケットの数。
Dropped X3 packets	このインターフェイスでドロップした ASR パケットの数。パケットは、パケットを転送しようとしたときにインターフェイスがダウン状態の場合にドロップされることがあります。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
delay	インターフェイスの遅延メトリックを変更します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

インターフェイスの IP アドレスおよびステータスを表示するには、特権 EXEC モードで **show interface ip brief** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドでは、VLAN インターフェイス、およびトランスペアレント モードでの管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内だけで指定できます。

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip brief** コマンドの出力例を示します。

```
hostname# show interface ip brief
```

```
Interface                  IP-Address      OK? Method  Status                Protocol
Control0/0                 127.0.1.1       YES CONFIG  up                    up
GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
GigabitEthernet0/1         unassigned      YES unset   administratively down down
GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
Management0/0              209.165.201.3   YES CONFIG  up
```

表 26-15 に、各フィールドの説明を示します。

表 26-15　show interface ip brief の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。すべてのインターフェイスを表示する場合、AIP SSM の内部インターフェイスに関する情報が表示されます（ASA 適応型セキュリティ アプライアンスに取り付けられている場合）。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
IP-Address	インターフェイスの IP アドレス。
OK?	このカラムは現在使用されておらず、常に「Yes」と表示されます。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。
Status	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Protocol	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show inventory

Product Identifier（PID; 製品 ID）、Version Identifier（VID; バージョン ID）、および Serial Number（SN; シリアル番号）が割り当てられているネットワーキング デバイスにインストールされているすべてのシスコ製品に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show inventory** コマンドを使用します。シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得または表示されません。

show inventory [**slot**]

構文の説明

slot	（任意）SSM スロット番号を指定します（システムはスロット 0）。

デフォルト

インベントリを表示するスロットを指定しない場合は、次のように処理されます。

- 電源を含めて、すべての SSM のインベントリ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	セマンティックに小さな変更が加えられました。

使用上のガイドライン

show inventory コマンドを使用すると、各シスコ製品に関するインベントリ情報が取得され、UDI 形式で表示されます。UDI は、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）という 3 つの別個のデータ要素を結合したものです。

PID は、製品の注文に使用する名前です。歴史的には、「製品名」または「部品番号」と呼ばれていました。これは、正確な交換部品を注文するために使用する ID です。

VID は製品のバージョンです。製品が改訂されるたびに、VID は増加します。VID は、製品変更の通知を管理する業界のガイドラインである、Telcordia GR-209-CORE から取得された厳格なプロセスに従って増加されます。

SN はベンダー固有の製品の通し番号です。それぞれの製造済み製品には、現場では変更できない固有のシリアル番号が工場で割り当てられます。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

UDI では各製品をエンティティと呼びます。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。各エンティティは、シスコ エンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワーキング デバイスに取り付けられており、PID が割り当てられているシスコ エンティティのリストが表示されます。

例

次に、キーワードまたは引数を指定していない **show inventory** コマンドの出力例を示します。この出力例では、ルータにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されています。

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC   , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999
```

表 26-16 は、この出力で表示されるフィールドについて説明しています。

表 26-16　show inventory フィールドの説明

フィールド	説明
Name	シスコ エンティティに割り当てられた物理名（テキスト ストリング）。たとえば、デバイスの物理コンポーネント命名構文に応じた「1」などのコンソールまたは簡易コンポーネントの番号（ポートまたはモジュールの番号）。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトを特徴付けるシスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。
VID	エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	エンティティのシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

関連コマンド

コマンド	説明
show diag	ネットワーキング デバイスのコントローラ、インターフェイス プロセッサ、およびポート アダプタについての診断情報を表示します。
show tech-support	ルータが問題を報告したときに、ルータに関する一般情報を表示します。

show ip address

インターフェイス IP アドレス（トランスペアレント モードの場合は管理 IP アドレス）を表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス IP アドレスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドに、VLAN インターフェイス用のサポートが追加されました。

使用上のガイドライン

このコマンドは、ハイ アベイラビリティに設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

例

次に、**show ip address** コマンドの出力例を示します。

```
hostname# show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

```
Current IP Addresses:
Interface               Name          IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz           209.165.200.225 255.255.255.224   manual
```

表 26-17 に、各フィールドの説明を示します。

表 26-17　show ip address の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。
Name	**nameif** コマンドで設定されたインターフェイス名。
IP address	インターフェイスの IP アドレス。
Subnet mask	IP アドレスのサブネット マスク。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

インターフェイスに対する DHCP リースまたはサーバに関する詳細情報を表示するには、特権 EXEC モードで **show ip address dhcp** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
server	DHCP サーバに関する情報を表示します。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいサーバ機能に対応するように **lease** および **server** キーワードが追加されました。
7.2(1)	このコマンドでは、VLAN インターフェイス、およびトランスペアレント モードでの管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip address dhcp lease** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
```

```
DHCP Transaction id:0x4123
Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
Temp default-gateway addr:209.165.201.1
Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
Next timer fires after:111797 secs
Retry count:0, Client-ID:cisco-0000.0000.0000-outside
Proxy: TRUE  Proxy Network: 10.1.1.1
Hostname: device1
```

表 26-18 に、各フィールドの説明を示します。

表 26-18　show ip address dhcp lease の各フィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネット マスク。
DHCP Lease server	DHCP サーバ アドレス。
state	DHCP リースの状態で、次のとおりです。 • [Initial]：初期化状態で、セキュリティ アプライアンスがリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。 • [Selecting]：セキュリティ アプライアンスは 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。 • [Requesting]：セキュリティ アプライアンスは、要求を送信した送信先サーバからの応答を待機しています。 • Purging：クライアントが IP アドレスを解放したか、他のエラーが発生したため、セキュリティ アプライアンスはリースを削除します。 • [Bound]：セキュリティ アプライアンスは有効なリースを保持し、正常に動作しています。 • [Renewing]：セキュリティ アプライアンスはリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。 • [Rebinding]：セキュリティ アプライアンスは元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。 • [Holddown]：セキュリティ アプライアンスはリースを削除するプロセスを開始しました。 • [Releasing]：セキュリティ アプライアンスは IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。
DHCP transaction id	クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバによって使用される乱数。
Lease	DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。

表 26-18　show ip address dhcp lease の各フィールド （続き）

フィールド	説明
Rebind	セキュリティ アプライアンスが DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、セキュリティ アプライアンスが元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。セキュリティ アプライアンスは、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
Temp default-gateway addr	DHCP サーバによって指定されるデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルト スタティック ルート。
Next timer fires after	内部タイマーがトリガーするまでの秒数。
Retry count	セキュリティ アプライアンスがリースを設定しようとしているとき、このフィールドは、セキュリティ アプライアンスが DHCP メッセージの送信を試行した回数を示します。たとえば、セキュリティ アプライアンスが Selecting 状態の場合、この値はセキュリティ アプライアンスが探索メッセージを送信した回数を示します。セキュリティ アプライアンスが Requesting 状態の場合、この値はセキュリティ アプライアンスが要求メッセージを送信した回数を示します。
Client-ID	サーバとのすべての通信に使用したクライアント ID。
Proxy	このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 26-19 に、各フィールドの説明を示します。

表 26-19　show ip address dhcp server の各フィールド

フィールド	説明
DHCP server	このインターフェイスがリースを取得した DHCP サーバ アドレス。最上位エントリ（「ANY」）はデフォルト サーバで常に存在します。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は一般的に 1 です。VPN 用のプロキシを実行中のインターフェイスに対してサーバがアドレスを提供している場合、リースは複数となります。
Offers	サーバからのオファーの数。
Requests	サーバに送信された要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した拒否の数。
Releases	サーバに送信されたリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバ アドレス。
DNS1	DHCP サーバから取得したセカンダリ DNS サーバ アドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバ アドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバ アドレス。
Subnet	DHCP サーバから取得したサブネット アドレス。
DNS Domain	DHCP サーバから取得したドメイン。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address dhcp	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、特権 EXEC モードで **show ip address pppoe** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip address pppoe** コマンドの出力例を示します。

```
hostname# show ip address outside pppoe
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address ppoe	PPPoE サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

show ip audit count [**global** | **interface** *interface_name*]

構文の説明

global	（デフォルト）すべてのインターフェイスについての一致数を表示します。
interface *interface_name*	（任意）指定したインターフェイスについての一致数を表示します。

デフォルト

キーワードを指定しない場合、このコマンドは、すべてのインターフェイスについての一致数を表示します（**global**）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

監査ポリシーを作成するには、**ip audit name** コマンドを使用します。ポリシーを適用するには、**ip audit interface** コマンドを使用します。

例

次に、**show ip audit count** コマンドの出力例を示します。

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

関連コマンド

コマンド	説明
clear ip audit count	監査ポリシーのシグニチャ一致カウントをクリアします。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

show ip verify statistics

ユニキャスト RPF 機能が原因でドロップしたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。ユニキャスト RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

show ip verify statistics [interface *interface_name*]

構文の説明

interface *interface_name*	（任意）指定したインターフェイスの統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ips

AIP SSM で設定されている使用可能な IPS 仮想センサーをすべて表示するには、特権 EXEC モードで **show ips** コマンドを使用します。

show ips [**detail**]

構文の説明

detail	（任意）センサーの ID 番号と名前を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドは、システム実行スペースで入力するとすべての仮想センサーを表示しますが、コンテキスト実行スペース内ではコンテキストに割り当てられた仮想センサーのみ表示します。仮想センサーをコンテキストに割り当てることについては、**allocate-ips** コマンドを参照してください。

仮想センサーは IPS バージョン 6.0 以降で使用できます。

例

次に、**show ips** コマンドの出力例を示します。

```
hostname# show ips
Sensor name
------------
ips1
ips2
```

次に、**show ips detail** コマンドの出力例を示します。

```
hostname# show ips detail
Sensor name               Sensor ID
------------              ---------
ips1                      1
ips2                      2
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
ips	トラフィックを AIP SSM に迂回させます。

show ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。また、このコマンドの代替形式の **show crypto ipsec sa** も使用できます。

show ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

detail	（任意）表示されているものに対する詳細なエラー情報を表示します。
entry	（任意）IPSec SA をピア アドレスの順に表示します。
identity	（任意）IPSec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	（任意）指定されたクリプト マップの IPSec SA を表示します。
peer *peer-addr*	（任意）指定されたピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec SA が表示されます。

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

（注）　IPSec SA ポリシーに、フラグメンテーションは IPSec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーで、フラグメンテーションは IPSec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次の例をグローバル コンフィギュレーション モードで入力すると、def という名前のクリプト マップの IPSec SA が表示されます。

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
```

```
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 480
        IV size: 8 bytes
        replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
hostname(config)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry** に対する IPSec SA が表示されます。

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry detail** を使って、IPSec SA が表示されます。

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
```

```
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次に、キーワード **identity** を使った IPSec SA の例を示します。

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使った IPSec SA の例を示します。

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

IPSec SA の要約を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa summary** コマンドを使用します。

show ipsec sa summary

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IPSec SA の要約を次の接続タイプ別に表示する例を示します（グローバル コンフィギュレーション モードで入力）。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロード バランシング

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:           Peak IPSec SA's:
IPSec            :     2        Peak Concurrent SA  :    14
IPSec over UDP   :     2        Peak Concurrent L2L :     0
IPSec over NAT-T :     4        Peak Concurrent RA  :    14
IPSec over TCP   :     6
IPSec VPN LB     :     0
Total            :    14
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA を完全に削除するか、特定のパラメータに基づいて削除します。
show ipsec sa	IPSec SA のリストを表示します。
show ipsec stats	IPSec 統計情報のリストを表示します。

show ipsec stats

IPSec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec stats** コマンドを使用します。

show ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
IPsec Global Statistics	このセクションは、セキュリティ アプライアンスがサポートする IPsec トンネルの総数に関係します。
Active tunnels	現在接続されている IPsec トンネルの数。
Previous tunnels	接続されたことがある IPsec トンネルの数（アクティブなトンネルを含む）。
Inbound	このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。
Bytes	受信した暗号トラフィックのバイト数。
Decompressed bytes	圧縮解除が実行された後に受信された暗号トラフィックのバイト数（該当する場合）。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	受信された IPsec 暗号化パケットの数。
Dropped packets	受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。

出力 （続き）	説明 （続き）
Replay failures	受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。
Authentications	受信された IPsec 暗号化パケットについて実行された認証の成功数。
Authentication failures	受信された IPsec 暗号化パケットについて検出された認証の失敗数。
Decryptions	受信された IPsec 暗号化パケットについて実行された復号化の成功数。
Decryption failures	受信された IPsec 暗号化パケットについて検出された復号の失敗数。
Decapsulated fragments needing reassembly	再構築が必要な IP フラグメントを含む復号 IPSec パケットの数。
Outbound	このセクションは、IPsec トラフィックを介して送信される発信クリアテキスト トラフィックに関係します。
Bytes	IPsec トンネルを介して暗号化および送信されるクリアテキスト トラフィックのバイト数。
Uncompressed bytes	IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキスト トラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	IPsec トンネルを介して暗号化および送信されるクリアテキスト パケットの数。
Dropped packets	IPsec トンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキスト パケットの数。
Authentications	IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。
Authentication failures	IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。
Encryptions	IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。
Encryption failures	IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。
Fragmentation successes	発信 IPsec パケットの変換の一部として実行されたフラグメンテーション操作の成功数。
Pre-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragmentation failures	発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。

出力 （続き）	説明 （続き）
Pre-fragmentation failures	発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation failure	発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragments created	IPsec の変換の一部として作成されたフラグメントの数。
PMTUs sent	IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。
PMTUs recvd	IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。
Protocol failures	受信した不正な形式の IPsec パケットの数。
Missing SA failures	指定された IPsec セキュリティ アソシエーションが存在しない、要求された IPsec の動作の数。
System capacity failures	IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できない IPsec の動作の数。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
```

```
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPSec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show ipv6 access-list

IPv6 アクセス リストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセス リストは、セキュリティ アプライアンスを通過できる IPv6 トラフィックを決定します。

show ipv6 access-list [*id* [*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*]]

構文の説明

any	（任意）IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	（任意）特定のホストの IPv6 アドレス。指定した場合、指定されたホストについてのアクセス ルールのみが表示されます。
id	（任意）アクセス リストの名前。指定した場合、指定されたアクセス リストのみが表示されます。
source-ipv6-prefix /*prefix-length*	（任意）IPv6 ネットワーク アドレスおよびプレフィックス。指定した場合、指定された IPv6 ネットワークについてのアクセス ルールのみが表示されます。

デフォルト

すべての IPv6 アクセス リストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

例

次に、**show ipv6 access-list** コマンドの出力例を示します。inbound、tcptraffic、および outbound という名前の IPv6 アクセス リストが表示されています。

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
```

```
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを作成します。

show ipv6 interface

IPv6 用に設定されたインターフェイスのステータスを表示するには、特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

構文の説明

brief	各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。
if_name	（任意）**nameif** コマンドで指定された内部または外部のインターフェイス名。指定されたインターフェイスのステータスおよびコンフィギュレーションのみが表示されます。
prefix	（任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。プレフィックスは、IPv6 アドレスのネットワーク部分です。

デフォルト

すべての IPv6 インターフェイスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 interface** コマンドの出力は **show interface** コマンドと類似しています。インターフェイスのハードウェアが使用できる場合、インターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
```

```
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、**brief** キーワードを入力した **show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 mld traffic

Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタ情報を表示するには、特権 EXEC モードで **show ipv6 mld traffic** コマンドを使用します。

show ipv6 mld traffic

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 mld traffic コマンドを使用すると、予期される数の MLD メッセージが受信および送信されたかどうかをチェックできます。

show ipv6 mld traffic コマンドで提供される情報は次のとおりです。

- **Elapsed time since counters cleared**：カウンタがクリアされてからの経過時間。
- **Valid MLD Packets**：受信および送信された有効な MLD パケットの数。
- **Queries**：受信および送信された有効なクエリーの数。
- **Reports**：受信および送信された有効なレポートの数。
- **Leaves**：受信および送信された有効な脱退の数。
- **Mtraee packets**：受信および送信されたマルチキャスト トレース パケットの数。
- **Errors**：発生したエラーのタイプと数。

例

次に、**show ipv6 mld traffic** コマンドの出力例を示します。

```
hostname# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                   Received           Sent
Valid MLD Packets  1                  3
Queries            1                  0
```

```
Reports            0                  3
Leaves             0                  0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

関連コマンド

コマンド	説明
clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。

show ipv6 neighbor

IPv6 ネイバー探索キャッシュ情報を表示するには、特権 EXEC モードで **show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbor [*if_name* | *address*]

構文の説明

address	（任意）指定された IPv6 アドレスについてのみネイバー探索キャッシュ情報を表示します。
if_name	（任意）**nameif** コマンドで設定する、指定されたインターフェイス名についてのみキャッシュ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 neighbor コマンドで提供される情報は次のとおりです。

- **IPv6 Address**：ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age**：アドレスが到達可能と確認されてからの経過時間（分単位）。ハイフン（-）はスタティック エントリを示します。
- **Link-layer Addr**：MAC アドレス。アドレスが不明の場合、ハイフン（-）が表示されます。
- **State**：ネイバー キャッシュ エントリの状態。

（注） 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、**INCMP**（不完全）状態と **REACH**（到達可能）状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 ネイバー探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

  - **INCMP**：（不完全）エントリに対してアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。

- **REACH**：（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。**REACH** 状態になっている間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。
- **STALE**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。**STALE** 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。
- **DELAY**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。**DELAY** 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE**：到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認をアクティブに要求します。
- **????**：不明な状態。

次に、IPv6 ネイバー探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- **INCMP**：（不完全）このエントリのインターフェイスはダウンしています。
- **REACH**：（到達可能）このエントリのインターフェイスは動作しています。

- **Interface**

  アドレスに到達可能であったインターフェイス。

例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor inside
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e  REACH inside
3001:1::45a                               - 0002.7d1a.9472  REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
ipv6 neighbor	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 route** コマンドを使用します。

show ipv6 route

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show route** コマンドと類似しています。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- **Codes**：ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - **C**：接続済み
  - **L**：ローカル
  - **S**：スタティック
  - **R**：RIP 生成
  - **B**：BGP 生成
  - **I1**：ISIS L1：統合 IS-IS Level 1 生成
  - **I2**：ISIS L2：統合 IS-IS Level 2 生成
  - **IA**：ISIS エリア間：統合 IS-IS エリア間生成
- **fe80::/10**：リモート ネットワークの IPv6 プレフィックスを示します。
- **[0/0]**：カッコ内の最初の数値は情報ソースのアドミニストレーティブ ディスタンスです。2 番めの数値はルートのメトリックです。
- **via ::**：リモート ネットワークへの次のルータのアドレスを指定します。
- **inside**：指定されたネットワークへの次のルータに到達できるインターフェイスを指定します。

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブル アップデートおよびルート キャッシュ アップデートのデバッグ メッセージを表示します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 routers

オンリンク ルータから受信した IPv6 ルータ アドバタイズメント情報を表示するには、特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

show ipv6 routers [*if_name*]

構文の説明

if_name	（任意）情報を表示する対象となる、**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 traffic

IPv6 トラフィックの統計情報を表示するには、特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

show ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トラフィック カウンタをクリアするには、**clear ipv6 traffic** コマンドを使用します。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

関連コマンド

コマンド	説明
clear ipv6 traffic	ipv6 トラフィック カウンタをクリアします。

CHAPTER 27

show isakmp ipsec-over-tcp stats コマンド～ show route コマンド

show isakmp ipsec-over-tcp stats

IPsec over TCP の実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp ipsec-over tcp stats** コマンドを使用します。

show isakmp ipsec-over-tcp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp ipsec-over-tcp stats** コマンドが追加されました。
7.2(1)	**show isakmp ipsec-over-tcp stats** コマンドは廃止されました。代わりに、**show crypto isakmp ipsec-over-tcp stats** コマンドが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures

- Checksum errors
- Internal errors

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
hostname(config)# show isakmp ipsec-over-tcp stats
Global IPSec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp sa** コマンドを使用します。

show isakmp sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE ピア	タイプ	Dir	Rky	ステート
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE ピア	タイプ	Dir	Rky	ステート	暗号	ハッシュ	認証	ライフタイム
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
hostname(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp stats** コマンドを使用します。

show isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show kernel process

セキュリティ アプライアンスで実行されているアクティブなカーネル プロセスの現在のステータスを表示するには、特権 EXEC モードで **show kernel process** コマンドを使用します。

show kernel process

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
8.0(0)	このコマンドが導入されました。

使用上のガイドライン

show kernel process コマンドを使用して、セキュリティ アプライアンスで実行されているカーネルに関する問題をトラブルシューティングします。

show kernel process コマンドの出力は、コンソール出力内に並べて出力されます。

例

次に、show kernel process コマンドの出力例を示します。

```
hostname# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
hostname#
```

表 27-1 に、各フィールドの説明を示します。

表 27-1　show kernel process のフィールド

フィールド	説明
PID	プロセス ID。
PPID	親プロセス ID。
PRI	プロセスのプライオリティ。
NI	プライオリティの計算に使用されるナイス値。値は 19（最大ナイス値）～ -19（最小ナイス値）の範囲です。
VSIZE	仮想メモリのサイズ（バイト単位）。
RSS	プロセスの Resident Set Size（KB 単位）。
WCHAN	プロセスが待機しているチャネル。
STAT	プロセスの状態。 • R：実行中 • S：割り込み可能な待機状態でスリープ中 • D：割り込み不可能なディスク スリープで待機中 • Z：ゾンビ • T：トレースまたは停止（信号による） • P：ページング
RUNTIME	プロセスがユーザ モードまたはカーネル モードでスケジュールされている jiffy の数。実行時間は utime と stime の合計です。
COMMAND	プロセス名。

show local-host

ローカル ホストのネットワーク状態を表示するには、特権 EXEC モードで **show local-host** を使用します。

show local-host [*ip_address*] [**detail**] [**all**][**brief**] **[connection {tcp <start>[-<end>] | udp <start>[-<end>] | embryonic <start>[-<end>]}]**

構文の説明

all	（任意）セキュリティ アプライアンスに接続するローカル ホストと、セキュリティ アプライアンスから接続するローカル ホストを含みます。
brief	（任意）ローカル ホストに関する簡潔な情報を表示します。
connection	（任意）接続の数とタイプに基づいて、3 種類のフィルタ、tcp、udp、embryonic を表示します。これらのフィルタは個別に使用することも、組み合わせて使用することもできます。
detail	（任意）アクティブな xlate およびネットワーク接続の詳細情報を含めた、ローカル ホスト情報の詳細なネットワーク状態を表示します。
ip_address	（任意）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	ホスト制限があるモデルでは、このコマンドにより、外部インターフェイスと見なされるインターフェイスが表示されるようになりました。
7.2(4)	新しい 2 つのオプション、*connection* と *brief* が **show local-host** コマンドに追加され、出力が内部ホストの接続数でフィルタリングされるようになりました。

使用上のガイドライン

show local-host コマンドを使用すると、ローカル ホストのネットワーク状態を表示できます。ローカル ホストは、トラフィックをセキュリティ アプライアンスに送信するか、またはトラフィックを通じて転送する任意のホストに対して作成されます。

このコマンドを使用すると、ローカル ホストの変換スロットおよび接続スロットを表示できます。このコマンドでは、通常の変換状態および接続状態が適用されない場合に、**nat 0 access-list** コマンドで設定されたホストの情報が提供されます。

このコマンドでは、接続の制限数も表示されます。接続制限が設定されていない場合、値として 0 が表示され、制限は適用されません。

ホスト制限のあるモデルの場合、ルーテッド モードで、内部のホスト（ワーク ゾーンとホーム ゾーン）は、外部（インターネット ゾーン）と通信するときにのみ制限値にカウントされます。インターネット ホストは制限値にカウントされません。ワークとホームの間のトラフィックを開始するホストも、制限値にカウントされません。デフォルト ルートに関連付けられたインターフェイスは、インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイス上のホストが制限値にカウントされます。トランスペアレント モードでは、ホスト数が最小のインターフェイスがホスト制限値にカウントされます。

TCP 代行受信が設定されている場合に、SYN 攻撃が発生すると、**show local-host** コマンド出力では、代行受信された接続の数が使用回数に計上されます。このフィールドは通常、完全なオープン接続のみを表示します。

show local-host コマンド出力では、スタティック接続を使用するホストに対して最大初期接続の制限値（TCP 代行受信の水準点）が設定されている場合に、`TCP embryonic count to host counter` が使用されます。このカウンタは、他のホストからこのホストに向かう初期接続の合計を示します。この合計が設定された最大制限値を超過すると、このホストへの新規接続に TCP 代行受信が適用されます。

例

次に、**show local-host** コマンドの出力例を示します。

```
hostname# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

次に、ホスト制限のあるセキュリティ アプライアンスでの **show local-host** コマンドの出力例を示します。

```
hostname# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限があるがデフォルト ルートのないセキュリティ アプライアンスでの **show local-host** コマンドの出力例を示します。ホスト制限はすべてのインターフェイスに適用されます。デフォルト ルート インターフェイスは、デフォルト ルートまたはルートが使用するインターフェイスがダウンしている場合は検出できないことがあります。

```
hostname# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

次に、ホスト制限のないセキュリティ アプライアンスでの **show local-host** コマンドの出力例を示します。

```
hostname# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

次に、ローカル ホストのネットワーク状態を表示する例を示します。

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
```

```
Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

次に、少なくとも 4 つの udp 接続があり、同時に 1 ～ 10 の tcp 接続のあるすべてのホストを表示する例を示します。

```
hostname# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
        watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
        Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
        10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
        10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
        maximum active, 0 denied
```

次に、**brief** オプションを使用したローカル ホストのアドレスと接続カウンタの例を示します。

```
hostname# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited
        TCP embryonic count to host = 0
        TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

次に、*brief* と *connection* 構文を使用したときの出力例を示します。

```
hostname#show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

hostname# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

関連コマンド

コマンド	説明
clear local-host	**show local-host** コマンドによって表示されるローカル ホストからのネットワーク接続を解放します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show logging

バッファ内のログまたはその他のロギング設定を表示するには、特権 EXEC モードで **show logging** コマンドを使用します。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

構文の説明

all	（任意）すべてのシステム ログ メッセージ ID と、その ID が有効か無効かを表示します。
asdm	（任意）ASDM ロギング バッファの内容を表示します。
message	（任意）デフォルト以外のレベルにあるメッセージを表示します。メッセージ レベルを設定するには、**logging message** コマンドを参照してください。
queue	（任意）システム ログ メッセージ キューを表示します。
setting	（任意）ロギング設定を表示します。ロギング バッファは表示されません。
syslog_id	（任意）表示するメッセージ番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(2)	syslog サーバが SSL/TLS 接続を使用するように設定されているかどうかを示します。
8.0(5)	TCP またはセキュア ホスト サーバへの再接続を 1 分ごとに試行します。

使用上のガイドライン

logging buffered コマンドを使用している場合、キーワードなしの **show logging** コマンドからは、現在のメッセージ バッファと現在の設定が表示されます。

show logging queue コマンドを使用すると、次の情報を表示できます。

- キュー内のメッセージ数
- キュー内に記録されたメッセージの最大数
- 処理に利用できるブロック メモリがなかったために廃棄されたメッセージ数

（注）　0 は、設定するキュー サイズとして許容される数値であり、最大許容キュー サイズを表します。設定されたキュー サイズがゼロの場合、**show logging queue** コマンドの出力で実際のキューのサイズが表示されます。

例

次に、**show logging** コマンドの出力例を示します。

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

次に、セキュアな syslog サーバが設定されている場合の **show logging** コマンドの出力例を示します。

```
hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure
hostname(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
        Logging to management 10.65.71.31 tcp/7777 Connected
         Logging to management 10.76.11.35 tcp/2222 Not connected since Sat, 21 Feb 2009
23:30:09 UTC
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

次に、**show logging message all** コマンドの出力例を示します。

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

関連コマンド

コマンド	説明
logging asdm	ASDM へのロギングをイネーブルにします。
logging buffered	バッファへのロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging message	メッセージ レベルを設定したり、メッセージをディセーブルにします。
logging queue	ロギング キューを設定します。

show logging rate-limit

禁止されたシステム ログ メッセージを元の設定で表示するには、特権 EXEC モードで **show logging rate-limit** コマンドを使用します。

show logging rate-limit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

情報がクリアされると、ホストが接続を再確立するまで、何も表示されません。

例

次に、禁止されたシステム ログ メッセージを表示する例を示します。

```
hostname(config)# show logging rate-limit
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

show mac-address-table [*interface_name* | **count** | **static]**

構文の説明

count	（任意）ダイナミックおよびスタティック エントリの合計数を一覧します。
interface_name	（任意）MAC アドレス テーブル エントリを表示するインターフェイス名を指定します。
static	（任意）スタティック エントリのみを一覧します。

デフォルト

インターフェイスを指定しない場合、すべてのインターフェイス MAC アドレス エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table
interface          mac address       type       Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、内部インターフェイスの **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table inside
interface          mac address       type       Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show management-access

管理アクセスに設定された内部インターフェイスの名前を表示するには、特権 EXEC モードで show management-access コマンドを使用します。

show management-access

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます （インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます)。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show memory

物理メモリの最大量、およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示するには、特権 EXEC モードで **show memory** コマンドを使用します。

show memory [**detail**]

構文の説明

detail	（任意）空きメモリおよび割り当て済みシステム メモリの詳細ビューを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show memory コマンドで、物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量の要約を表示できます。メモリは必要に応じて割り当てられます。

show memory detail の出力を **show memory binsize** コマンドとともに使用して、メモリ リークをデバッグできます。

show memory detail コマンド出力は、要約、DMA メモリ、ヒープ メモリの 3 つのセクションに分割できます。要約には、メモリ全体がどのように割り当てられているかが表示されます。DMA にリンクしていないメモリ、または予約されていないメモリは、ヒープと見なされます。Free Memory というラベルのメモリは、ヒープ内の未使用のメモリです。Allocated memory in use の値は、割り当てられているヒープの量です。ヒープ割り当ての明細は、出力の後半で表示されます。予約メモリおよび DMA 予約メモリは、別のシステム プロセスおよび主に VPN サービスによって使用されます。

SNMP を使用して **show memory** コマンドから情報を表示することもできます。

例

この例では、物理メモリの最大量および現在使用可能な空きメモリ量の要約を表示します。

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

この例は、詳細なメモリ出力を表示します。

```
hostname# show memory detail
Free memory:                           130546920 bytes (49%)
Used memory:                           137888536 bytes (51%)
    Allocated memory in use:            33030808 bytes (12%)
    Reserved memory:                        65454208 bytes (24%)
    DMA Reserved memory:                    39403520 bytes (15%)
    -----------------------------      ----------------
Total memory:                          268435456 bytes (100%)
Dynamic Shared Objects(DSO):               0 bytes
DMA memory:
    Unused memory:                     3212128 bytes ( 8%)
    Crypto reserved memory:            2646136 bytes ( 7%)
        Crypto free:                   1605536 bytes ( 4%)
        Crypto used:                   1040600 bytes ( 3%)
    Block reserved memory:             33366816 bytes (85%)
        Block free:                    31867488 bytes (81%)
        Block used:                    1499328 bytes ( 4%)
    Used memory:                        178440 bytes ( 0%)
    -----------------------------      ----------------
    Total memory:                      39403520 bytes (100%)
    HEAP memory:
        Free memory:                   130546920 bytes (80%)
        Used memory:                   33030808 bytes (20%)
            Init used memory by library:  4218752 bytes ( 3%)
            Allocated memory:          28812056 bytes (18%)
    -----------------------------      ----------------
    Total memory:                      163577728 bytes (100%)

Least free memory:     122963528 bytes (75%)
Most used memory:      40614200 bytes (25%)

    ----- fragmented memory statistics -----

fragment size      count       total
    (bytes)                   (bytes)
---------------- ---------- --------------
       16         113        1808

<--- More --->
```

関連コマンド

コマンド	説明
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory app-cache

システム上のデータ パスなどの多くの主要アプリケーションで使用されるアプリケーションのキャッシュ データ構造の統計情報をリアルタムで表示するには、特権 EXEC モードで **show memory app-cache** コマンドを使用します。

show memory app-cache [threat-detection | host | flow | tcb] [detail]

構文の説明

flow	（任意）flow のアプリケーション レベル メモリ キャッシュを表示します。
host	（任意）host のアプリケーション レベル メモリ キャッシュを表示します。
tcb	（任意）tcb のアプリケーション レベル メモリ キャッシュを表示します。
threat-detection	（任意）threat-detection のアプリケーション レベル メモリ キャッシュを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(1)	このコマンドが導入されました。

使用上のガイドライン

show memory app-cache コマンドにより表示される情報は、アプリケーション キャッシュ処理の監視、メモリ リークのトラブルシューティング、およびマルチコア システムにおけるシステムのトラフィックの負荷分散の分析に役立ちます。

例

次は、**show memory app-cache** コマンドの出力例です。

```
hostname(config)# sh mem app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn chunk 700 0 24175 0 15181900
SNP Host Container 700 0 48330 0 6766200
SNP conn set counte 700 0 0 0 0
SNP APP ID chunk 700 0 0 0 0
SNP Run-time Inspec 700 0 0 0 0
SNP TCB chunk 700 0 36328 0 6539040
SNP MP PF Mod chunk 700 0 0 0 0
SNP MP SVC Conn chu 700 0 0 0 0
SNP SVC Session chu 700 0 0 0 0
SNP Midpath Service 700 0 0 0 0
SNP MP Stack chunk 700 0 1 0 364
CP APP ID chunk 700 0 0 0 0
SNP ACE statistics 50 0 0 0 0
SNP Host statistics 50 0 3732 0 26586768
SNP Subnet statisti 50 0 1796 0 3146592

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8550 0 114449 0 58220864

hostname(config)# sh mem app-cache threat-detection d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP ACE statistics 50 0 0 0 0
SNP Host statistics 50 50 50 0 356200
SNP Subnet statisti 50 50 50 0 87600

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 150 100 100 0 443800

hostname(config)# sh mem app-cache host d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Container 700 700 700 0 98000

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 98000

hostname(config)# sh mem app-cache flow d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn chunk 700 700 700 0 439600

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 439600

hostname(config)# sh mem app-cache tcb d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB chunk 700 700 700 0 126000

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 126000
```

関連コマンド

コマンド	説明
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレス範囲を表示します。

コマンド	説明
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory binsize

特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示するには、特権 EXEC モードで **show memory binsize** コマンドを使用します。

show memory binsize *size*

構文の説明

size	特定のバイナリ サイズのチャンク（メモリ ブロック）を表示します。バイナリ サイズは **show memory detail** コマンド出力の「fragment size」カラムから取得されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、バイナリ サイズ 500 に割り当てられたチャンクについての要約情報を表示する例を示します。

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

関連コマンド

コマンド	説明
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレス範囲を表示します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。

show memory delayed-free-poisoner

memory delayed-free-poisoner キューの使用状況の要約を表示するには、特権 EXEC モードで **show memory delayed-free-poisoner** コマンドを使用します。

show memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドを使用して、キューおよび統計情報をクリアします。

例

次に、**show memory delayed-free-poisoner** コマンドの出力例を示します。

```
hostname# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
        3335600:  memory held in queue
           6095:  current queue count
              0:  elements dequeued
              3:  frees ignored by size
           1530:  frees ignored by locking
             27:  successful validate runs
              0:  aborted validate runs
       01:09:36:  local time of last validate
```

表 27-2 に、**show memory delayed-free-poisoner** コマンド出力での重要なフィールドの説明を示します。

表 27-2　show memory delayed-free-poisoner コマンド出力の説明

フィールド	説明
memory held in queue	delayed free-memory poisoner ツール キューに保留されたメモリ。delayed free-memory poisoner ツールがイネーブルになっていない場合、このようなメモリは、通常、**show memory** 出力では「空き」容量になります。
current queue count	キューにある要素の数。
elements dequeued	キューから削除された要素の数。この数は、システム内の空きメモリだったメモリの大部分またはすべてが最終的にキューに保持されることになった場合に増加し始めます。
frees ignored by size	要求が小さすぎて必要なトラッキング情報を保持できなかったため、キューに配置されなかった解放要求の数。
frees ignored by locking	複数のアプリケーションがメモリを使用しているため、キューに配置されずに、ツールによって代行受信された解放要求の数。最後にメモリを解放してシステムに戻したアプリケーションが、このメモリ領域をキューに割り当てます。
successful validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、キューの内容が（自動的に、または **memory delayed-free-poisoner validate** コマンドによって）検証された回数。
aborted validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、またはクリアされた後で、複数のタスク（定期的な実行または CLI からの検証要求）が同時にキューを使用しようとしたため、キューの内容をチェックする要求が中止された回数。
local time of last validate	最後の検証の実行が完了したときのローカル システム時刻。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。

show memory profile

セキュリティ アプライアンス のメモリ使用率（プロファイリング）に関する情報を表示するには、特権 EXEC モードで **show memory profile** コマンドを使用します。

show memory profile [peak] [detail | collated | status]

構文の説明

collated	（任意）表示されるメモリ情報を整形します。
detail	（任意）メモリの詳細情報を表示します。
peak	（任意）「使用中」のバッファではなく、ピーク キャプチャ バッファを表示します。
status	（任意）メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show memory profile コマンドを使用して、メモリ使用状況レベルとメモリ リークをトラブルシューティングします。プロファイリングが停止されている場合でも、プロファイル バッファの内容を表示できます。プロファイリングを開始すると、バッファは自動的にクリアされます。

（注） メモリ プロファイリングをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスが一時的に低下する場合があります。

例

次に例を示します。

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

次に示す **show memory profile detail** コマンドの出力は、6 つのデータ カラムと 1 つのヘッダー カラムに区分され、左揃えで表示されています。ヘッダー カラムには、先頭のデータ カラムに対応するメモリ バケットのアドレスが表示されます（16 進値）。データ自体は、バケット アドレスにあるテキ

ストまたはコードが保持しているバイト数です。データ カラム内のピリオド（.）は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケット アドレスを表しています。たとえば、最初の行の先頭のデータ カラムのアドレス バケットは 0x001069e0 です。最初の行の 2 番めのデータ カラムのアドレス バケットは 0x001069e4 で、以降も同様に増分していきます。通常は、ヘッダー カラムにあるアドレスが次のバケット アドレスです。これは、前の行の最後のデータ カラムのアドレスに増分値を加算したものです。使用状況が含まれない行は表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダー カラムに 3 個のピリオド（...）で示されます。

```
hostname# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

次に、整形された出力の例を示します。

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<snip>
```

次に、ピーク キャプチャ バッファの例を示します。

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次に、ピーク キャプチャ バッファと、対応するバケット アドレスにあるテキストまたはコードが保持しているバイト数の例を示します。

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

次に、メモリ プロファイリングの現在の状態とピーク キャプチャ バッファの例を表示します。

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。

show memory tracking

ツールによって追跡される、現在割り当て済みのメモリを表示するには、特権 EXEC モードで show memory tracking コマンドを実行します。

show memory tracking [address | dump | detail]

構文の説明

address	（任意）アドレスごとのメモリのトラッキングを表示します。
detail	（任意）内部メモリのトラッキング状態を表示します。
dump	（任意）メモリ トラッキング アドレスのダンプを出力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0（8）	このコマンドが導入されました。

使用上のガイドライン

show memory tracking コマンドを使用して、ツールにより追跡されている、現在割り当て済みのメモリを表示します。

例

次に、**show memory tracking** コマンドの出力例を示します。

```
hostname# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

次に、**show memory tracking address** と **show memory tracking dump** の出力例を示します。

```
hostname# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

```
memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2

hostname# memory tracking dump 0xa893aed0
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | .................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | .................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | .................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。
show memory tracking	現在割り当てられているメモリを表示します。

show memory webvpn

webvpn のメモリ使用状況の統計情報を生成するには、特権 EXEC モードで **show memory webvpn** コマンドを使用します。

show memory webvpn [allobjects | blocks | dumpstate [cache | disk0 | disk1 | flash | ftp | system | tftp]| pools | profile [clear | dump | start | stop] | usedobjects {{begin | exclude | grep | include} line *line*}]

構文の説明

allobjects	プール、ブロック、すべての使用済みオブジェクトおよび解放済みオブジェクトについて、webvpn メモリ使用量の詳細を表示します。
begin	一致する行から開始します。
blocks	メモリ ブロックについて、webvpn メモリ使用量の詳細を表示します。
cache	webvpn メモリ キャッシュ状態のダンプのファイル名を指定します。
clear	webvpn メモリ プロファイルをクリアします。
disk0	webvpn メモリ disk0 状態のダンプのファイル名を指定します。
disk1	webvpn メモリ disk1 状態のダンプのファイル名を指定します。
dump	webvpn メモリ プロファイルをファイルに出力します。
dumpstate	webvpn メモリ状態をファイルに出力します。
exclude	一致する行を除外します。
flash	webvpn メモリ フラッシュ状態のダンプのファイル名を指定します。
ftp	webvpn メモリ ftp 状態のダンプのファイル名を指定します。
grep	一致する行を含めるか、または除外します。
include	一致する行を含めます。
line	一致する行を特定します。
line	一致する行を指定します。
pools	メモリ プールについて、webvpn メモリ使用量の詳細を表示します。
profile	webvpn メモリ プロファイルを収集して、ファイルに出力します。
system	webvpn メモリ システム状態のダンプのファイル名を指定します。
start	webvpn メモリ プロファイルの収集を開始します。
stop	webvpn メモリ プロファイルの収集を停止します。
tftp	webvpn メモリ tftp 状態のダンプのファイル名を指定します。
usedobjects	使用済みオブジェクトについて、webvpn メモリ使用量の詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例　次に、**show memory webvpn allobjects** コマンドの出力例を示します。

```
hostname# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

関連コマンド

コマンド	説明
memory-size	WebVPN が使用できるセキュリティ アプライアンスのメモリ量を設定します。

show memory-caller address

セキュリティ アプライアンス に設定されたアドレス範囲を表示するには、特権 EXEC モードで **show memory-caller address** コマンドを使用します。

show memory-caller address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アドレス範囲を **show memory-caller address** コマンドで表示する前に、**memory caller-address** コマンドで設定する必要があります。

例

次に、**memory caller-address** コマンドで設定したアドレス範囲、および **show memory-caller address** コマンドによる表示結果の例を示します。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

アドレス範囲が **show memory-caller address** コマンドを入力する前に設定されていなかった場合、アドレスは表示されません。

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

関連コマンド

コマンド	説明
memory caller-address	発信元 PC のメモリ ブロックを設定します。

show mfib

転送エントリおよびインターフェイスの観点から MFIB を表示するには、特権 EXEC モードで **show mfib** コマンドを使用します。

show mfib [*group* [*source*]] [**verbose**]

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。
verbose	（任意）エントリに関する追加情報を表示します。

デフォルト

任意の引数を指定しないと、すべてのグループの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib** コマンドの出力例を示します。

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib verbose	転送エントリおよびインターフェイスに関する詳細情報を表示します。

show mfib active

アクティブなマルチキャスト送信元を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib active** コマンドを使用します。

show mfib [*group*] **active** [*kbps*]

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
kbps	（任意）この値以上のマルチキャスト ストリームのみに表示を制限します。

デフォルト

kbps のデフォルト値は 4 です。*group* を指定しない場合、すべてのグループが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show mfib active コマンドの出力では、PPS のレートに正または負の数値が表示されます。セキュリティ アプライアンスが負の数値を表示するのは、RPF パケットが失敗した場合か、ルータが発信インターフェイス（OIF）リストを使用して RPF パケットをモニタしている場合です。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

例

次に、**show mfib active** コマンドの出力例を示します。

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

関連コマンド

コマンド	説明
show mroute active	アクティブなマルチキャスト ストリームを表示します。

show mfib count

MFIB ルートとパケット数データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib count** コマンドを使用します。

show mfib [*group* [*source*]] **count**

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、パケットのドロップに関する統計情報を表示します。

例

次に、**show mfib count** コマンドの出力例を示します。

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

関連コマンド

コマンド	説明
clear mfib counters	MFIB ルータ パケット カウンタをクリアします。
show mroute count	マルチキャスト ルート カウンタを表示します。

show mfib interface

MFIB プロセスに関係しているインターフェイスのパケット統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib interface** コマンドを使用します。

show mfib interface [*interface*]

構文の説明

interface	（任意）インターフェイス名。指定されたインターフェイスのみに表示を制限します。

デフォルト

すべての MFIB インターフェイスの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib interface** コマンドの出力例を示します。

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib reserved

予約済みグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib reserved** コマンドを使用します。

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

構文の説明

count	（任意）パケットおよびルートの数に関するデータを表示します。
verbose	（任意）追加情報を表示します。
active	（任意）アクティブなマルチキャスト送信元を表示します。
kpbs	（任意）この値以上のアクティブなマルチキャスト送信元のみに表示を制限します。

デフォルト

kbps のデフォルト値は 4 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、224.0.0.0 ～ 224.0.0.225 の範囲の MFIB エントリを表示します。

例

次に、**show mfib reserved** コマンドの出力例を示します。

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
```

```
inside Flags: IC
```

関連コマンド

コマンド	説明
show mfib active	アクティブなマルチキャスト ストリームを表示します。

show mfib status

MFIB の全般的なコンフィギュレーションと動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib status** コマンドを使用します。

show mfib status

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib status** コマンドの出力例を示します。

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib summary

MFIB のエントリとインターフェイスの数に関する要約情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib summary** コマンドを使用します。

show mfib summary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib summary** コマンドの出力例を示します。

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

関連コマンド

コマンド	説明
show mroute summary	マルチキャスト ルーティング テーブルの要約情報を表示します。

show mfib verbose

転送エントリとインターフェイスに関する詳細情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib verbose** コマンドを使用します。

show mfib verbose

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib verbose** コマンドの出力例を示します。

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show mfib summary	MFIB のエントリとインターフェイスの数に関する要約情報を表示します。

show mgcp

MGCP のコンフィギュレーションとセッション情報を表示するには、特権 EXEC モードで **show mgcp** コマンドを使用します。

show mgcp {**commands** | **sessions**} [**detail**]

構文の説明

commands	コマンド キュー内の MGCP コマンドの数を表示します。
sessions	既存の MGCP セッションの数を表示します。
detail	（任意）各コマンド（またはセッション）に関する追加情報を出力に表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド（またはセッション）に関する追加情報を出力に含めます。

例

次に、**show mgcp** コマンド オプションの例を示します。

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
hostname#

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP|host-pc-2
        Transaction ID  2052
        Endpoint name|aaln/1
        Call ID|9876543210abcdef
        Connection ID|
        Media IP|192.168.5.7
        Media port|6058
hostname#
```

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
hostname#

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
hostname#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug mgcp	MGCP のデバッグ情報をイネーブルにします。
inspect mgcp	MGCP アプリケーション インスペクションをイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。

show mmp

既存の MMP セッションに関する情報を表示するには、特権 EXEC モードで **show mmp** コマンドを使用します。

show mmp [*address*]

構文の説明

address	MMP クライアント/サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、既存の MMP セッションに関する情報を表示する **show mmp** コマンドの使用例を示します。

```
hostname# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

関連コマンド

コマンド	説明
debug mmp	MMP 検査イベントを表示します。
inspect mmp	MMP インスペクション エンジンを設定します。
show debug mmp	MMP インスペクション モジュールの現在のデバッグ設定を表示します。

show mode

実行中のソフトウェア イメージ、およびフラッシュ メモリ内の任意のイメージのためのセキュリティ コンテキスト モードを表示するには、特権 EXEC モードで **show mode** コマンドを使用します。

show mode

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mode** コマンドの出力例を示します。次に、現在のモードと、実行されていないイメージ「image.bin」のモードの例を示します。

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

モードは、マルチまたはシングルのいずれかです。

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
mode	コンテキスト モードをシングルまたはマルチに設定します。

show module

ASA 5500 シリーズ適応型セキュリティ アプライアンスの SSM に関する情報やシステムの情報を表示するには、ユーザ EXEC モードで **show module** コマンドを使用します。

show module [**all** | *slot* [**details** | **recover**]]

構文の説明

all	（デフォルト）スロット 1 の SSM とスロット 0 のシステムに関する情報を表示します。
details	（任意）インテリジェント SSM（たとえば ASA-SSM-*x*0 など）のリモート管理コンフィギュレーションを含む、追加情報を表示します。
recover	（任意）インテリジェント SSM について、**hw-module module recover** コマンドの設定を表示します。 **（注）** **recover** キーワードが有効になるのは、**hw-module module recover** コマンドに **configure** キーワードを使用して SSM のリカバリ コンフィギュレーションを作成した場合のみです。
slot	（任意）スロット番号として 0 または 1 を指定します。スロット 0 は、セキュリティ アプライアンスの基本システムです。

デフォルト

両方のスロットの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、より多くの詳細情報を出力するように変更されました。

使用上のガイドライン

このコマンドでは、SSM および、システムと組み込みインターフェイスに関する情報を示します。

show module recover コマンドは、システム実行スペースでのみ使用できます。

例

次に、**show module** コマンドの出力例を示します。スロット 0 は基本システムで、スロット 1 は CSC SSM です。

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
```

```
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

表 22 に、各フィールドの説明を示します。

表 27-3　show module のフィールド

フィールド	説明
Mod	スロット番号（0 または 1）。
Card Type	スロット 0 に表示されるシステムの場合、タイプはプラットフォーム モデルです。スロット 1 の SSM の場合、タイプは SSM タイプです。
Model	このスロットのモデルです。
Serial No.	シリアル番号。
MAC Address Range	この SSM 上のインターフェイス、またはデバイス、組み込みインターフェイスの MAC アドレス範囲。
Hw Version	ハードウェアのバージョン。
Fw Version	ファームウェアのバージョン。
Sw Version	ソフトウェアのバージョン。
SSM Application Name	SSM で実行されているアプリケーションの名前。
SSM Application Version	SSM で実行されているアプリケーションのバージョン。
Status	スロット 0 のシステムの場合、ステータスは Up Sys です。スロット 1 の SSM のステータスは、次のいずれかです。 • Initializing：SSM が検出され、システムによってコントロール通信が初期化されます。 • Up：SSM がシステムによる初期化を完了しました。 • Unresponsive：この SSM との通信中にシステムでエラーが発生しました。 • Reloading：インテリジェント SSM の場合、SSM をリロードしています。 • Shutting Down：SSM をシャットダウンしています。 • Down：SSM がシャットダウンされました。 • Recover：インテリジェント SSM の場合、SSM がリカバリ イメージをダウンロードしようとしています。

表 27-3　show module のフィールド （続き）

フィールド	説明
Data Plane Status	SSM へのデータ プレーンの現在の状態。
Compatibility	残りのシステムに関連した SSM の互換性。

show module details コマンドの出力は、スロットにある SSM のタイプによって異なります。たとえば、CSC SSM の出力には CSC SSM ソフトウェアのコンポーネントに関するフィールドが含まれます。これらのフィールドは、スロットに AIP SSM がある場合には表示されません。次に、**show module details** コマンドの出力例を示します。

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

表 23 に、各フィールドの説明を示します。**show module** コマンドでも表示されるフィールドについては、表 22 を参照してください。

表 27-4　show module details フィールド

フィールド	説明
Mgmt IP addr	インテリジェント SSM の場合、SSM 管理インターフェイスの IP アドレスを表示します。
Mgmt web ports	インテリジェント SSM の場合、管理インターフェイスに設定されたポートを表示します。
Mgmt TLS enabled	インテリジェント SSM の場合、SSM の管理インターフェイスの接続に対してトランスポート層のセキュリティがイネーブルであるかどうか（True または False）を示します。

次に、**show module** コマンドに **recover** キーワードが使用された場合の出力例を示します。

```
hostname> show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。

show mrib client

MRIB クライアント接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib client** コマンドを使用します。

show mrib client [**filter**] [**name** *client_name*]

構文の説明

filter	（任意）クライアント フィルタを表示します。各クライアントが所有する MRIB フラグと、各クライアントが関連するフラグに関する情報を表示するために使用します。
name *client_name*	（任意）PIM または IGMP など、MRIB のクライアントとして動作するマルチキャスト ルーティング プロトコルの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

filter オプションを使用して、さまざまな MRIB クライアントが登録されているルートおよびインターフェイス レベル フラグの変更を表示します。このコマンド オプションからは、MRIB クライアントが所有するフラグも表示されます。

例

次に、**filter** キーワードを使用した **show mrib client** コマンドの出力例を示します。

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
```

```
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルのエントリを表示します。

show mrib route

MRIB テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib route** コマンドを使用します。

show mrib route [[*source* | *****] [*group*[/*prefix-length*]]]

構文の説明

*	（任意）共有ツリー エントリを表示します。
/*prefix-length*	（任意）MRIB ルートのプレフィックス長。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
group	（任意）グループの IP アドレスまたは名前。
source	（任意）ルート送信元の IP アドレスまたは名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

MFIB テーブルには、MRIB から更新されるエントリとフラグのサブセットが保持されます。フラグは、マルチキャスト パケットの転送ルールのセットに従って、転送およびシグナリングの動作を決定します。

インターフェイスとフラグのリストに加えて、各ルート エントリにはさまざまなカウンタが表示されます。バイト数は、転送されたバイトの合計数です。パケット数は、このエントリについて受信されたパケット数です。**show mfib count** コマンドは、ルートとは無関係にグローバルなカウンタを表示します。

例

次に、**show mrib route** コマンドの出力例を示します。

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
```

```
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

関連コマンド

コマンド	説明
show mfib count	MFIB テーブルのルートとパケット数データを表示します。
show mrib route summary	MRIB テーブル エントリの要約を表示します。

show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、特権 EXEC モードで **show mroute** コマンドを使用します。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

構文の説明

active *rate*	（任意）アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定された *rate* 以上で送信を実行している送信元です。*rate* が指定されていない場合、アクティブな送信元は 4 kbps 以上のレートで送信を実行している送信元です。
count	（任意）グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。
group	（任意）DNS ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。
pruned	（任意）プルーニングされたルートを表示します。
reserved	（任意）予約済みグループを表示します。
source	（任意）送信元のホスト名または IP アドレス。
summary	（任意）マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。

デフォルト

rate 引数を指定しない場合、デフォルトでは 4 Kbps になります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show mroute コマンドは、マルチキャスト ルーティングの内容を表示します。セキュリティ アプライアンスは、PIM プロトコル メッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して、マルチキャスト ルーティング テーブルにデータを入力します。アスタリスク（*）はすべての送信元アドレス、「S」は単一の送信元アドレス、「G」は宛先マルチキャスト グループ アドレスを意味します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で（RPF を経由して）見つかった宛先グループへの最適パスを使用します。

実行コンフィギュレーションに含まれている **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**show mroute** コマンドの出力例を示します。

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute の出力には、次のフィールドが含まれています。

- **Flags**：エントリに関する情報を提供します。
  - **D（Dense）**：エントリはデンス モードで動作しています。
  - **S（Sparse）**：エントリはスパース モードで動作しています。
  - **B（Bidir Group）**：マルチキャスト グループが双方向モードで動作していることを示します。
  - **s（SSM Group）**：マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
  - **C（Connected）**：マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
  - **L（Local）**：セキュリティ アプライアンス自体が、マルチキャスト グループのメンバーです。グループは、（設定済みのグループに対する）**igmp join-group** コマンドによってローカルに加入されています。
  - **I（Received Source Specific Host Report）**：(S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。
  - **P（Pruned）**：ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。
  - **R（RP-bit set）**：(S,G) エントリが RP をポイントしていることを示します。
  - **F（Register flag）**：ソフトウェアがマルチキャスト送信元に登録されていることを示します。
  - **T（SPT-bit set）**：パケットが最短パス送信元ツリーで受信されていることを示します。
  - **J（Join SPT）**：(*, G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します （デフォルトの SPT しきい値設定は 0 Kbps です）。J - Join 最短パス ツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S, G) パケットが受信されると、送信元の方向に (S, G) join がトリガーされます。これにより、セキュリティ アプライアンスは送信元ツリーに加入します。

(S, G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、セキュリティ アプライアンスは送信元ツリー上のトラフィック速度をモニタします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとします。

（注）　セキュリティ アプライアンスは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*, G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*, G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、セキュリティ アプライアンスは最短パス送信元ツリーにただちに切り替えます。

- **Timers:Uptime/Expires** : Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
- **Interface state** : 着信インターフェイスまたは発信インターフェイスの状態を示します。
  - **Interface** : 着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。
  - **State** : アクセス リストまたは Time to Live（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。
- **(*, 239.1.1.40)** と **(* , 239.2.2.1)** : IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元を意味します。
- **RP** : RP のアドレス。スパース モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 224.0.0.0 です。
- **Incoming interface** : 送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- **RPF nbr** : 送信元に対するアップストリーム ルータの IP アドレス。
- **Outgoing interface list** : パケット転送時に使用されるインターフェイス。

関連コマンド

コマンド	説明
clear configure mroute	実行コンフィギュレーションから **mroute** コマンドを削除します。
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	設定されているマルチキャスト ルートを表示します。

show nac-policy

NAC ポリシーの使用状況の統計およびグループ ポリシーに対する NAC ポリシーの割り当てを表示するには、特権 EXEC モードで **show nac-policy** コマンドを使用します。

show nac-policy [*nac-policy-name*]

構文の説明

nac-policy-name	（任意）使用状況の統計を表示する対象の NAC ポリシー名。

デフォルト

名前を指定しない場合は、すべての NAC ポリシー名がそれぞれの統計情報とともに CLI に一覧表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、framework1 および framework2 という名前の NAC ポリシーのデータの例を示します。

```
asa2(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

各 NAC ポリシーの 1 行めは、名前とタイプ（nac-framework）を示します。ポリシーがどのグループ ポリシーにも割り当てられていない場合は、CLI のポリシー タイプの隣に「is not in use」というテキストが表示されます。それ以外は、そのグループ ポリシーの使用状況データが CLI に表示されます。表 27-5 に、**show nac-policy** コマンドのフィールドの説明を示します。

表 27-5　show nac-policy コマンドのフィールド

フィールド	説明
applied session count	このセキュリティ アプライアンスが NAC ポリシーを適用した VPN セッションの累積数。

表 27-5　show nac-policy コマンドのフィールド （続き）

フィールド	説明
applied group-policy count	このセキュリティ アプライアンスが NAC ポリシーを適用したグループ ポリシーの累積数。
group-policy list	NAC ポリシーが割り当てられているグループ ポリシーのリスト。この場合、グループ ポリシーの使用状況によってこのリストに表示されるかどうかは決まりません。NAC ポリシーが実行コンフィギュレーションのグループ ポリシーに割り当てられている場合は、このリストにグループ ポリシーが表示されます。

関連コマンド

clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	IPSec、Cisco WebVPN、および NAC の各セッションの数を表示します。

show nameif

nameif コマンドを使用して設定されているインターフェイス名を表示するには、特権 EXEC モードで show nameif コマンドを使用します。

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

構文の説明

mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス名を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内だけで指定できます。このコマンドの出力では、Interface カラムにはマッピング名のみが示されます。

例

次に、**show nameif** コマンドの出力例を示します。

```
hostname# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show nat

NAT ポリシー カウンタを表示するには、特権 EXEC モードで **show nat** コマンドを使用します。

show nat *src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

構文の説明

dst_ifc	（任意）フィルタリングする宛先インターフェイスを指定します。
dst_ip	（任意）フィルタリングする宛先 IP アドレスを指定します。
dst_mask	（任意）宛先 IP アドレスのマスクを指定します。
src_ifc	（任意）フィルタリングする送信元インターフェイスを指定します。
src_ip	（任意）フィルタリングする送信元 IP アドレスを指定します。
src_mask	（任意）送信元 IP アドレスのマスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

static、**nat**、または **alias** コマンドが設定されている場合、該当するインターフェイス間で NAT ポリシーに内部的に変換されます。**show nat** コマンドは、変換または変換解除が実行されたときに検索されるポリシーを表示します。

NAT ポリシーの出力は次の情報で構成されています。

- 合致させる必要があるトラフィックの match 句。
- 合致の後に実行する、次のいずれかのアクション。
  - static 変換
  - エイリアス変換
  - アイデンティティ NAT
  - NAT 免除
  - 変換グループが見つからない場合の暗黙の拒否
- カウンタ：translate_hits は、実アドレスからマッピングされたアドレスへの変換のカウンタを提供し、untranslate_hits はマッピングされたアドレスから実アドレスへの変換のカウンタを提供します。

例

次に、**show nat** コマンドの出力例を示します。

```
hostname(config)# show nat

NAT policies on Interface inside:
  match ip inside host 172.16.1.1 outside any
    static translation to 209.165.200.224
    translate_hits = 0, untranslate_hits = 0

NAT policies on Interface management:
  match ip management any outside 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any test 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any management 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any outside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any test any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any management any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
```

関連コマンド

コマンド	説明
clear nat counters	NAT ポリシー カウンタをクリアします。
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
nat-control	NAT コンフィギュレーション要件をイネーブルまたはディセーブルにします。
nat-rewrite	DNS 応答の A レコードに埋め込まれた IP アドレスの NAT リライトをイネーブルにします。

show ntp associations

NTP アソシエーション情報を表示するには、ユーザ EXEC モードで **show ntp associations** コマンドを使用します。

show ntp associations [**detail**]

構文の説明

detail	（任意）各アソシエーションの追加情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show ntp associations** コマンドの出力例を示します。

```
hostname> show ntp associations
     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

表 27-6 に、各フィールドの説明を示します。

表 27-6　show ntp associations のフィールド

フィールド	説明
（表示行の行頭文字）	表示行の行頭には、次の文字が 1 つまたはそれ以上表示されます。 • *：このピアに同期しています。 • #：このピアに対してほぼ同期しています。 • +：ピアは同期可能な対象として選択されています。 • -：ピアが選択候補です。 • ～：ピアがスタティックに設定されていますが、同期していません。
address	NTP ピアのアドレス。
ref clock	ピアのリファレンス クロックのアドレス。
st	ピアの層。
when	ピアから最終 NTP パケットが受信されてからの時間。
poll	ポーリング間隔（秒）。
reach	ピアの到達可能性（8 進のビット ストリング）。
delay	ピアまでのラウンド トリップ遅延（ミリ秒）。
offset	ローカル クロックに対するピア クロックの相対時間（ミリ秒）。
disp	分散値。

次に、**show ntp associations detail** コマンドの出力例を示します。

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

表 27-7 に、各フィールドの説明を示します。

表 27-7　show ntp associations detail のフィールド

フィールド	説明
IP-address configured	サーバ（ピア）の IP アドレス。
（ステータス）	• our_master：セキュリティ アプライアンスがこのピアに対して同期しています。 • selected：ピアは同期可能な対象として選択されています。 • candidate：ピアが選択候補です。

表 27-7　show ntp associations detail のフィールド （続き）

フィールド	説明
（健全性）	• sane：ピアが基本健全性チェックをパスしました。 • insane：ピアが基本健全性チェックで失敗しました。
（有効性）	• valid：ピア時間は有効であると見なされています。 • invalid：ピア時間は無効であると見なされています。 • leap_add：ピアが、うるう秒が加算されることをシグナリングしています。 • leap-sub：ピアが、うるう秒が減算されることをシグナリングしています。
stratum	ピアの層。
（リファレンス ピア）	unsynced：ピアは、他のどのマシンにも同期されていません。 ref ID：ピアの同期対象となるマシンのアドレス。
time	ピアがマスターから受信した最終タイムスタンプ。
our mode client	ピアに対する相対的なモード。常に「クライアント」です。
peer mode server	ピアの相対的なモード。常に「サーバ」です。
our poll intvl	ピアに対するポーリング間隔。
peer poll intvl	ピアからのポーリング間隔。
root delay	ルートへのパスに沿った遅延（最上位ストラタム 1 の時刻源）。
root disp	ルートへのパスの分散。
reach	ピアの到達可能性（8 進のビット ストリング）。
sync dist	ピアの同期間隔。
delay	ピアまでのラウンド トリップ遅延。
offset	クロックに相対的なピア クロックのオフセット。
dispersion	ピア クロックの分散。
precision	ピア クロックの精度（ヘルツ）。
version	ピアが使用中の NTP バージョン番号。
org time	開始時のタイムスタンプ。
rcv time	受信時のタイムスタンプ。
xmt time	送信時のタイムスタンプ。
filtdelay	各サンプルのラウンド トリップ遅延（ミリ秒）。
filtoffset	各サンプルのクロック オフセット（ミリ秒）。
filterror	各サンプルの誤差の概算値。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show ntp status

各 NTP アソシエーションのステータスを表示するには、ユーザ EXEC モードで **show ntp status** コマンドを使用します。

show ntp status

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show ntp status** コマンドの出力例を示します。

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

表 27-8 に、各フィールドの説明を示します。

表 27-8　show ntp status のフィールド

フィールド	説明
Clock	• synchronized：セキュリティ アプライアンスが NTP サーバに対して同期しています。 • unsynchronized：セキュリティ アプライアンスが NTP サーバに対して同期していません。
stratum	このシステムの NTP ストラタム。
reference	セキュリティ アプライアンスの同期対象になる NTP サーバのアドレス。

表 27-8　show ntp status のフィールド （続き）

フィールド	説明
nominal freq	システム ハードウェア クロックの公称周波数。
actual freq	システム ハードウェア クロックの測定周波数。
precision	このシステムのクロックの精度（ヘルツ）。
reference time	リファレンス タイムスタンプ。
clock offset	同期されたピアに対するシステム クロックのオフセット。
root delay	ルート クロックまでのパスに沿った合計遅延。
root dispersion	ルート パスの分散。
peer dispersion	同期されたピアの分散。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。

show ospf

OSPF ルーティング プロセスに関する一般情報を表示するには、特権 EXEC モードで **show ospf** コマンドを使用します。

show ospf [*pid* **[***area_id***]**]

構文の説明

area_id	（任意）OSPF アドレス範囲に関連付けられているエリアの ID。
pid	（任意）OSPF プロセスの ID。

デフォルト

pid を指定しない場合は、すべての OSPF プロセスが一覧表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

pid を指定すると、指定したルーティング プロセスの情報のみが含まれます。

例

次に、**show ospf** コマンドの出力例を示します。ここでは、特定の OSPF ルーティング プロセスに関する一般情報を表示する例を示しています。

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

次に、**show ospf** コマンドの出力例を示します。ここでは、すべての OSPF ルーティング プロセスに関する一般情報を表示する例を示しています。

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
```

```
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf border-routers

ABR および ASBR に対する内部 OSPF ルーティング テーブル エントリを表示するには、特権 EXEC モードで **show ospf border-routers** コマンドを使用します。

show ospf border-routers

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**ospf border-routers** コマンドの出力例を示します。

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf database

セキュリティ アプライアンス上の OSPF トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show ospf database** コマンドを使用します。

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

構文の説明

addr	（任意）ルータのアドレス。
adv-router	（任意）アドバタイズされたルータ。
area_id	（任意）OSPF アドレス範囲に関連付けられているエリアの ID。
asbr-summary	（任意）ASBR リストの要約を表示します。
database	データベース情報を表示します。
database-summary	（任意）データベース全体の要約リストを表示します。
external	（任意）指定した自律システムの外部のルートを表示します。
internal	（任意）指定した自律システム内部のルート。
lsid	（任意）LSA ID。
network	（任意）ネットワークに関する OSPF データベース情報を表示します。
nssa-external	（任意）外部の Not-So-Stubby Area リストを表示します。
pid	（任意）OSPF プロセスの ID。
router	（任意）ルータを表示します。
self-originate	（任意）指定した自律システムに関する情報を表示します。
summary	（任意）リストの要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf database** コマンドの出力例を示します。

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

次に、**show ospf database asbr-summary** コマンドの出力例を示します。

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

次に、**show ospf database router** コマンドの出力例を示します。

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

次に、**show ospf database network** コマンドの出力例を示します。

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

次に、**show ospf database summary** コマンドの出力例を示します。

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次に、**show ospf database external** コマンドの出力例を示します。

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf flood-list

インターフェイスを介してフラッディングされるのを待機している OSPF LSA のリストを表示するには、特権 EXEC モードで **show ospf flood-list** コマンドを使用します。

show ospf flood-list *interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf flood-list** コマンドの出力例を示します。

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf interface

OSPF 関連のインターフェイス情報を表示するには、特権 EXEC モードで **show ospf interface** コマンドを使用します。

show ospf interface [*interface_name*]

構文の説明

interface_name	（任意）OSPF 関連の情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

interface_name 引数を指定せずに使用すると、すべてのインターフェイスの OSPF 情報が表示されます。

例

次に、**show ospf interface** コマンドの出力例を示します。

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開きます。

show ospf neighbor

インターフェイスごとの OSPF ネイバー情報を表示するには、特権 EXEC モードで **show ospf neighbor** コマンドを使用します。

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

構文の説明

detail	（任意）指定したルータに関する詳細な情報を表示します。
interface_name	（任意）ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	（任意）隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show ospf neighbor** コマンドの出力例を示します。ここでは、インターフェイスごとの OSPF ネイバー情報を表示する例を示しています。

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
neighbor	非ブロードキャスト ネットワークに相互接続する OSPF ルータを設定します。
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf request-list** コマンドを使用します。

show ospf request-list *nbr_router_id interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。このインターフェイスからルータによって要求されたすべての LSA のリストを表示します。
nbr_router_id	隣接ルータのルータ ID。このネイバーからルータによって要求されたすべての LSA のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show ospf request-list** コマンドの出力例を示します。

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

関連コマンド

コマンド	説明
show ospf retransmission-list	再送信を待機しているすべての LSA のリストを表示します。

show ospf retransmission-list

再送信されるのを待機しているすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf retransmission-list** コマンドを使用します。

show ospf retransmission-list *nbr_router_id interface_name*

構文の説明

interface_name	ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

nbr_router_id 引数を指定すると、このネイバーの、再送信されるのを待機しているすべての LSA のリストが表示されます。

interface_name 引数を指定すると、このインターフェイスの、再送信されるのを待機しているすべての LSA のリストが表示されます。

例

次に、**show ospf retransmission-list** コマンドの例を示します。例では、*nbr_router_id* 引数は 192.168.1.11 で、*if_name* 引数は outside です。

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

関連コマンド

コマンド	説明
show ospf request-list	ルータによって要求されたすべての LSA のリストを表示します。

show ospf summary-address

OSPF プロセスに対して設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、特権 EXEC モードで **show ospf summary-address** コマンドを使用します。

show ospf summary-address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show ospf summary-address** コマンドの出力例を示します。この例は、ID が 5 である OSPF プロセスに対してサマリー アドレスが設定される前に、すべてのサマリー アドレス再配布情報のリストを表示する方法を示しています。

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

関連コマンド

コマンド	説明
summary-address	OSPF の集約アドレスを作成します。

show ospf virtual-links

OSPF 仮想リンクのパラメータと現在の状態を表示するには、特権 EXEC モードで **show ospf virtual-links** コマンドを使用します。

show ospf virtual-links

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show ospf virtual-links** コマンドの出力例を示します。

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

関連コマンド

コマンド	説明
area virtual-link	OSPF 仮想リンクを定義します。

show perfmon

セキュリティ アプライアンスのパフォーマンスに関する情報を表示するには、特権 EXEC モードで **show perfmon** コマンドを使用します。

show perfmon [**detail**]

構文の説明

detail	（任意）追加の統計情報を表示します。これらの統計情報は Cisco Unified Firewall MIB のグローバル接続オブジェクトとプロトコルごとの接続オブジェクトにより収集された情報と一致します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。
7.2(1)	**detail** キーワードが追加されました。

使用上のガイドライン

このコマンドの出力は、Telnet セッションには表示されません。

perfmon コマンドでは、指定した間隔でパフォーマンス統計情報が連続的に表示されます。**show perfmon** コマンドを使用すると、すぐに情報を表示できます。

例

次に、**show perfmon** コマンドの出力例を示します。

```
hostname(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
```

```
AAA Authen            0/s           0/s
AAA Author            0/s           0/s
AAA Account           0/s           0/s
```

次に、**show perfmon detail** コマンドの出力例を示します。

```
hostname(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s           0/s
Connections          0/s           0/s
TCP Conns            0/s           0/s
UDP Conns            0/s           0/s
URL Access           0/s           0/s
URL Server Req       0/s           0/s
TCP Fixup            0/s           0/s
HTTP Fixup           0/s           0/s
FTP Fixup            0/s           0/s
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
TCP Intercept        0/s           0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

関連コマンド

コマンド	説明
perfmon	指定した間隔で詳細なパフォーマンス モニタ情報を表示します。

show phone-proxy

phone-proxy 固有の情報を表示するには、グローバル コンフィギュレーション モードで **show phone-proxy** コマンドを使用します。

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

構文の説明

detail	詳細情報を表示します。
media-sessions	電話プロキシによって保存されている、対応するメディア セッションを表示します。
secure-phones	データベースに格納されているセキュア モードに対応した電話を表示します。
signaling-sessions	電話プロキシに保存されている、対応するシグナリング セッションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**show phone proxy** コマンドを使用して電話プロキシ固有の情報を表示する例を示します。

```
hostname(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
hostname(config)#
```

次に、**show phone proxy** コマンドを使用して、データベースに保存されている、セキュア モードに対応した電話を表示します。

```
hostname(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
hostname(config)#
```

次に、show phone proxy コマンドを使用して、正常に行われたコールからの出力を表示する例を示します。

```
hostname(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

関連コマンド

コマンド	説明
debug phone-proxy	電話プロキシ インスタンスからのデバッグ メッセージを表示します。
phone proxy	Phone Proxy インスタンスを設定します。

show pim df

ランデブー ポイント（RP）またはインターフェイスについて、双方向 DF の「勝者」を表示するには、ユーザ EXEC または特権 EXEC モードで **show pim df** コマンドを使用します。

show pim df [**winner**] [*rp_address* | *if_name*]

構文の説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
if_name	インターフェイスの物理名または論理名。
winner	（任意）DF 選出の勝者をインターフェイスごと、RP ごとに表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RP への勝者のメトリックも表示します。

例

次に、**show pim df** コマンドの出力例を示します。

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

グループからプロトコルへのマッピング テーブルを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim group-map** コマンドを使用します。

show pim group-map [**info-source**] [*group*]

構文の説明

group	（任意）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
info-source	（任意）グループ範囲情報の情報源を表示します。

デフォルト

すべてのグループについて、グループからプロトコルへのマッピングを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RP について、グループとプロトコルとのアドレス マッピングをすべて表示します。マッピングは、セキュリティ アプライアンス上でさまざまなクライアントから学習されます。

セキュリティ アプライアンスの PIM 実装は、さまざまな特殊エントリをマッピング テーブルで保持しています。Auto-rp グループ範囲は、スパース モード グループ範囲から明確に拒否されます。SSM グループ範囲もスパース モードには入りません。リンクローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も、スパース モード グループ範囲から拒否されます。最後のエントリは、所定の RP でスパース モードに入っている残りすべてのグループを示します。

pim rp-address コマンドで複数の RP を設定した場合は、適切なグループ範囲が対応する RP とともに表示されます。

例

次に、**show pim group-map** コマンドの出力例を示します。

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
```

```
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

1 行めと 2 行めで、Auto-RP グループ範囲がスパース モード グループ範囲から明確に拒否されています。

3 行めでは、リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.255。224.0.0.0/24 として定義）もスパース モード グループ範囲から拒否されています。

4 行めでは、PIM 送信元特定マルチキャスト（PIM-SSM）グループ範囲が 232.0.0.0/8 にマッピングされています。

最後のエントリは、残りすべてのグループがスパース モードに入って、RP 10.10.3.2 にマッピングされたことを示しています。

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。
pim rp-address	PIM ランデブー ポイント（RP）のアドレスを設定します。

show pim interface

PIM に関するインターフェイス固有の情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim interface** コマンドを使用します。

show pim interface [*if_name* | **state-off** | **state-on**]

構文の説明

if_name	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
state-off	（任意）PIM がディセーブルになっているインターフェイスを表示します。
state-on	（任意）PIM がイネーブルになっているインターフェイスを表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する PIM 情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、このコマンドの出力にあるネイバー数カラムでは、ネイバー数が実際の数よりも 1 つ多く表示されます。

例

次に、内部インターフェイスに関する PIM 情報を表示する例を示します。

```
hostname# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

show pim join-prune statistic

PIM の加入とプルーニングに関する集約的な統計情報を表示するには、ユーザ EXEC モードと特権 EXEC モードで **show pim join-prune statistics** コマンドを使用します。

show pim join-prune statistics [*if_name*]

構文の説明

if_name	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて、加入とプルーニングに関する統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM の加入とプルーニングに関する統計情報をクリアするには、**clear pim counters** コマンドを使用します。

例

次に、**show pim join-prune statistic** コマンドの出力例を示します。

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim neighbor

PIM ネイバー テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim neighbor** コマンドを使用します。

show pim neighbor [**count** | **detail**] [*interface*]

構文の説明

interface	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
count	（任意）PIM ネイバーの合計数、および各インターフェイスの PIM ネイバーの数を表示します。
detail	（任意）upstream-detection hello オプションを通じて学習した、ネイバーの追加アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、このルータが PIM の hello メッセージを通じて学習した PIM ネイバーを特定するために使用します。また、このコマンドは、インターフェイスが Designated Router（DR; 指定ルータ）であること、およびネイバーで双方向処理が可能になるタイミングも示します。

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、セキュリティ アプライアンス インターフェイスがこのコマンドの出力に表示されます。セキュリティ アプライアンスの IP アドレスは、アドレスの次にアスタリスク（*）を付けて示されています。

例

次に、**show pim neighbor** コマンドの出力例を示します。

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

show pim range-list

PIM の範囲リストの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim range-list** コマンドを使用します。

show pim range-list [*rp_address*]

構文の説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、マルチキャスト転送モードからグループへのマッピングを特定するために使用されます。出力には、この範囲のランデブー ポイント（RP）のアドレスも示されます（該当する場合）。

例

次に、**show pim range-list** コマンドの出力例を示します。

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

関連コマンド

コマンド	説明
show pim group-map	グループから PIM モードへのマッピング、およびアクティブな RP の情報を表示します。

show pim topology

PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology [*group*] [*source*]

構文の説明

group	（任意）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
source	（任意）次のいずれかを指定できます。 • マルチキャスト送信元の名前。DNS の hosts テーブルに定義されているものか、**ipv4 host** コマンドで定義したものです。 • マルチキャスト送信元の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。

デフォルト

すべてのグループと送信元のトポロジ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM トポロジ テーブルは、所定のグループのさまざまなエントリ、(*, G)、(S, G)、(S, G)RPT をそれぞれのインターフェイス リストとともに表示するために使用します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、インターネット グループ管理プロトコル（IGMP）などのローカル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

MRIB は、所定の (S, G) エントリについて、どのインターフェイスでデータ パケットを受け取る必要があるか、どのインターフェイスでデータ パケットを転送する必要があるかを示します。また、転送時には Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）テーブルを使用して、パケットごとの転送アクションを決定します。

（注）　転送情報を表示するには、**show mfib route** コマンドを使用します。

例

次に、**show pim topology** コマンドの出力例を示します。

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルを表示します。
show pim topology reserved	予約済みグループの PIM トポロジ テーブルの情報を表示します。

show pim topology reserved

予約済みグループに関する PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology reserved** コマンドを使用します。

show pim topology reserved

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show pim topology reserved** コマンドの出力例を示します。

```
hostname# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside             00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside              00:00:48  off II
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim topology route-count

PIM トポロジ テーブルのエントリの数を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology route-count [**detail**]

構文の説明

detail	（任意）グループごとに、数に関する詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルのエントリの数を表示します。エントリに関する詳細な情報を表示するには、**show pim topology** コマンドを使用します。

例

次に、**show pim topology route-count** コマンドの出力例を示します。

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim traffic

PIM トラフィックのカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim traffic** コマンドを使用します。

show pim traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM トラフィックのカウンタをクリアするには、**clear pim counters** コマンドを使用します。

例

次に、**show pim traffic** コマンドの出力例を示します。

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim tunnel

PIM トンネル インターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim tunnel** コマンドを使用します。

show pim tunnel [*if_name*]

構文の説明

if_name	（任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて PIM トンネル情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM レジスタ パケットは、仮想カプセル化トンネル インターフェイスを経由して、送信元の最初のホップ DR ルータから RP に送信されます。RP では、仮想カプセル化解除トンネルを使用して、PIM レジスタ パケットの受信インターフェイスを表現します。このコマンドは、両方のタイプのインターフェイスについてトンネル情報を表示します。

レジスタ トンネルは、（PIM レジスタ メッセージ内に）カプセル化された、送信元からのマルチキャスト パケットです。送信元は、共有ツリーを経由して、配布のために RP に送信されます。登録が適用されるのは、SM に対してのみです。SSM および双方向 PIM には適用されません。

例

次に、**show pim tunnel** コマンドの出力例を示します。

```
hostname# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show power inline

ASA 5505 適応型セキュリティ アプライアンスなどの PoE インターフェイスを持つモデルでインターフェイス上の電源ステータスを表示するには、ユーザ EXEC モードで **show power inline** コマンドを使用します。

show power inline

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PoE インターフェイスを使用して、IP フォンまたはワイヤレス アクセス ポイントなどの電源を必要するデバイスを接続します。

例

次に、**show power inline** コマンドの出力例を示します。

```
hostname> show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

表 27-9 に、各フィールドの説明を示します。

表 27-9　show power inline のフィールド

フィールド	説明
Interface	セキュリティ アプライアンス上のすべてのインターフェイスを表示します。PoE が使用できないインターフェイスも含みます。
Power	電源が On か Off かを示します。デバイスに電源が必要でない場合、インターフェイスにデバイスがない場合、またはインターフェイスがシャットダウンしている場合、値は Off になります。インターフェイスが PoE をサポートしていない場合、値は n/a です。
Device	給電されるデバイスのタイプを表示します。Cisco または IEEE のいずれかです。デバイスが給電されていない場合、値は n/a です。デバイスの給電が Cisco の場合、ディスプレイには Cisco と表示されます。IEEE は、デバイスの給電が IEEE 802.3af 準拠であることを示します。

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show priority-queue statistics

インターフェイスのプライオリティ キューに関する統計情報を表示するには、特権 EXEC モードで **show priority-queue statistics** コマンドを使用します。

show priority-queue statistics [*interface-name*]

構文の説明

interface-name	（任意）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合は、すべての設定済みインターフェイスについてプライオリティ キュー統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、test というインターフェイスについて **show priority-queue statistics** コマンドを使用した場合のコマンド出力を示しています。この出力で、BE はベストエフォート キュー、LLQ は低遅延キューを表しています。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
clear priority-queue statistics	特定のインターフェイス、またはすべての設定済みインターフェイスに関するプライオリティ キュー統計情報のカウンタをクリアします。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

show processes

セキュリティ アプライアンス上で動作しているプロセスのリストを表示するには、特権 EXEC モードで **show processes** コマンドを使用します。

show processes [cpu-usage | *non-zero* **|** *sorted***] [cpu-hog | memory | internals]**

構文の説明

non-zero	（任意）CPU 使用状況がゼロではないプロセスを表示します。
sorted	（任意）プロセスの CPU 使用状況をソートして表示します。

デフォルト

デフォルトで、このコマンドはセキュリティ アプライアンスで実行されているプロセスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがサポートされるようになりました。
7.0(4)	Runtime 値が拡張され、1 ミリ秒以内の精度で表示されるようになりました。
7.2(1)	出力表示が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。
8.0(1)	**show process cpu-usage** 引数が追加されました。

使用上のガイドライン

show processes コマンドを使用すると、セキュリティ アプライアンス上で実行されているプロセスのリストを表示できます。

また、オプションの **cpu-usage or cpu-hog** 引数によって、CPU を使用しているプロセスを特定できます。CPU を 100 ミリ秒を超えて占有している場合、プロセスにフラグが設定されます。

show process cpu-usage コマンドは、セキュリティ アプライアンス上で実行されているプロセスと、5 秒間、1 分間、5 分間の CPU 使用状況の統計情報を表示します。セキュリティ アプライアンスの管理者はこのコマンドを使用して、セキュリティ アプライアンスの CPU を使用している可能性があるセキュリティ アプライアンス上の特定のプロセスに絞り込むことができます。追加された引数 *sorted* および *non-zero* を使用して、コマンド出力をさらにカスタマイズできます。

show process cpu-hog コマンドを呼び出すと、次のカラムが表示されます。

- MAXHOG：CPU 占有実行の最長期間（ミリ秒単位）。
- NUMHOG：CPU 占有実行の回数。
- LASTHOG：最後の CPU 占有実行の期間（ミリ秒単位）。
- PC：CPU 占有プロセスの命令ポインタ。
- Traceback：CPU 占有プロセスのスタック トレース。

プロセスは、数個の命令だけを必要とする軽量スレッドです。リスト内で、PC はプログラム カウンタ、SP はスタック ポインタ、STATE はスレッド キューのアドレス、Runtime はスレッドが CPU クロック サイクルに基づいて実行されている時間（ミリ秒）、SBASE はスタックのベース アドレス、Stack は現在使用されているバイト数と合計サイズであり、Process はスレッドの機能を示します。

ランタイム値を 1 ミリ秒以内の精度で表示するように強化され、クロック ティック（精度 10 ミリ秒）の代わりに CPU クロック サイクル（< 10 ナノ秒の精度）に基づいた CPU 使用状況のプロセスのアカウンティングが正確で完全になりました。

Traceback には最大で 14 のアドレスを設定できます。

スケジューラと合計サマリー行で、**show proccess** コマンドを 2 回連続で実行し、その出力を比較して次のことを判断できます。

- CPU 時間がどこで 100 % 使用されたか。
- 各スレッドが CPU を何 % 使用しているか。これは、スレッドのランタイム差分を合計ランタイム差分と比較して判断します。

オプションの **memory** 引数を指定すると、各プロセスによって割り当てられたメモリが表示されます。

オプションの **internals** 引数を指定すると、起動されたコールの数とギブアップの数が表示されます。Invoked は、スケジューラがプロセスを起動した（実行した）回数です。Giveups は、プロセスが CPU をスケジューラに返還した回数です。

例

次に、セキュリティ アプライアンス上で動作しているプロセスのリストを表示する例を示します。

```
hostname(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total

hostname(config)# show proc cpu-usage non-zero
PC          Thread      5Sec    1Min    5Min    Process
0818af8e    d482f92c    0.1%    0.1%    0.1%    Dispatch Unit
08bae136    d48180f0    0.1%    0.0%    0.2%    ssh
---------------------------------------

hostname(config)# show processes cpu

Process: ci/console, NUMHOG: 1, MAXHOG: 210, LASTHOG: 210 LASTHOG At:  01:08:24 UTC Jul 24
2005
PC:          153412
Traceback:    1532de  15352a  14b66d  14ba61 148c30 14930e  1125d1
```

```
Process: fover_parse, NUMHOG: 2, MAXHOG: 200, LASTHOG: 200
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           6ff434
Traceback:    6ff838  6fe3a7  6fe424  6fe5ab 7060b7 3bfa44  1125d1

hostname(config)# show processes memory

------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)


hostname# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

show reload

セキュリティ アプライアンスのリロードのステータスを表示するには、特権 EXEC モードで **show reload** コマンドを使用します。

show reload

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次の例では、リロードが 4 月 20 日土曜日の午前 12:00（深夜）に スケジュールされていることを示します。

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

関連コマンド

コマンド	説明
reload	コンフィギュレーションをリブートおよびリロードします。

show resource allocation

すべてのクラスとクラス メンバーにまたがってリソースごとにリソース割り当てを表示するには、特権 EXEC モードで **show resource allocation** コマンドを使用します。

show resource allocation [**detail**]

構文の説明

detail	追加情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況を表示するには、**show resource usage** コマンドを使用します。

例

次に、**show resource allocation** コマンドの出力例を示します。ディスプレイには、各リソースの合計割り当て値が、絶対値および使用可能なシステム リソースのパーセンテージとして表示されます。

```
hostname# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 All                    unlimited
```

表 27-10 に、各フィールドの説明を示します。

表 27-10　show resource allocation のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	使用できる場合は、すべてのコンテキストで割り当てられるシステム リソース総量のパーセンテージ。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
hostname# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
```

```
                bronze              0      CA          5
                All Contexts:       3                          20     20.00%

Xlates          default           all      CA  unlimited
                gold                1      DA  unlimited
                silver              1      CA      23040      23040     N/A
                bronze              0      CA      11520
                All Contexts:       3                      23040     N/A

mac-addresses   default           all       C      65535
                gold                1       D      65535      65535   100.00%
                silver              1      CA       6553       6553     9.99%
                bronze              0      CA       3276
                All Contexts:       3                     137623   209.99%
```

表 27-11 に、各フィールドの説明を示します。

表 27-11　show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Class	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 セキュリティ アプライアンスでは、「A」を「C」または「D」と組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	使用できる場合、クラス内のすべてのコンテキストにわたって割り当てられるシステム リソースの合計数のパーセンテージ。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。

コマンド	説明
show resource types	制限を設定できるリソース タイプを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

show resource types

セキュリティ アプライアンスが使用状況の追跡対象にしているリソース タイプを表示するには、特権 EXEC モードで **show resource types** コマンドを使用します。

show resource types

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは、コンテキストごとに管理できる追加のリソース タイプを表示するように変更されました。

例

次に、リソース タイプの例を示します。

```
hostname# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

関連コマンド

コマンド	説明
clear resource usage	リソース使用状況の統計情報をクリアします。
context	セキュリティ コンテキストを追加します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

show resource usage

セキュリティ アプライアンスまたはマルチ モードの各コンテキストのリソース使用状況を表示するには、特権 EXEC モードで **show resource usage** コマンドを使用します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**]
[**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

構文の説明

context *context_name*	（マルチ モードのみ）統計情報を表示するコンテキストの名前を指定します。すべてのコンテキストを対象にするには、**all** を指定します。セキュリティ アプライアンスは、各コンテキストのリソース使用状況を一覧表示します。
count_threshold	表示するリソースの使用回数を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。 **（注）** すべてのリソースを表示するには、*count_threshold* を **0** に設定します。
counter *counter_name*	次のカウンタ タイプの数を表示します。 • **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。 • **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。 • **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。 • **all**：（デフォルト）すべての統計情報を表示します。
detail	管理できないリソースを含むすべてのリソースのリソース使用状況を表示します。たとえば、TCP 代行受信の数を表示できます。

resource [**rate**] *resource_name*	特定のリソースの使用状況を表示します。すべてのリソースを対象にするには、**all**（デフォルト）を指定します。リソースの使用状況を表示するには、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM 管理セッション。 • **conns**：1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション インスペクション。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **mac-addresses**：トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチ モードのみ）すべてのコンテキストの合算使用状況を表示します。
system	（マルチ モードのみ）すべてのコンテキストの合算使用状況を表示します。ただし、コンテキストの合算制限値ではなくシステムのリソース制限値を表示します。
top *n*	（マルチ モードのみ）指定したリソースの上位 *n* 人のユーザのコンテキストを表示します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。

デフォルト

マルチ コンテキスト モードでは、デフォルト コンテキストは **all** です。すべてのコンテキストのリソース使用状況が表示されます。シングル モードの場合、コンテキスト名は無視され、出力では「context」は「System」として表示されます。

デフォルトのリソース名は、**all** です。すべてのリソース タイプが表示されます。

デフォルトのカウンタ名は、**all** です。すべての統計情報が表示されます。

デフォルトのカウントしきい値は **1** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	コンテキストごとにリソースを制限できるようになったため、このコマンドは現在では拒否されたリソースを表示します

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。ここでは、すべてのコンテキストのリソース使用状況が表示されますが、合算のコンテキスト制限値ではなくシステム制限値が表示されています。

```
hostname# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

次に、**show resource usage detail counter all 0** コマンドの出力例を示します。このコマンドは、ユーザが管理できるリソースだけでなく、すべてのリソースを表示します。

```
hostname# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
```

```
chunk:dhcp-lease-s          0           0  unlimited           0 admin
chunk:dnat                  0           0  unlimited           0 admin
chunk:ether                 0           0  unlimited           0 admin
chunk:est                   0           0  unlimited           0 admin

...

Telnet                      0           0          5           0 admin
SSH                         1           1          5           0 admin
ASDM                        0           1          5           0 admin
Syslogs [rate]              0          68  unlimited           0 admin
aaa rate                    0           0  unlimited           0 admin
url filter rate             0           0  unlimited           0 admin
Conns                       1           6  unlimited           0 admin
Xlates                      0           0  unlimited           0 admin
tcp conns                   0           0  unlimited           0 admin
Hosts                       2           3  unlimited           0 admin
udp conns                   0           0  unlimited           0 admin
smtp-fixups                 0           0  unlimited           0 admin
Conns [rate]                0           7  unlimited           0 admin
establisheds                0           0  unlimited           0 admin
pps                         0           0  unlimited           0 admin
syslog rate                 0           0  unlimited           0 admin
bps                         0           0  unlimited           0 admin
Fixups [rate]               0           0  unlimited           0 admin
non tcp/udp conns           0           0  unlimited           0 admin
tcp-intercepts              0           0  unlimited           0 admin
globals                     0           0  unlimited           0 admin
np-statics                  0           0  unlimited           0 admin
statics                     0           0  unlimited           0 admin
nats                        0           0  unlimited           0 admin
ace-rules                   0           0        N/A           0 admin
aaa-user-aces               0           0        N/A           0 admin
filter-rules                0           0        N/A           0 admin
est-rules                   0           0        N/A           0 admin
aaa-rules                   0           0        N/A           0 admin
console-access-rul          0           0        N/A           0 admin
policy-nat-rules            0           0        N/A           0 admin
fixup-rules                 0           0        N/A           0 admin
aaa-uxlates                 0           0  unlimited           0 admin
CP-Traffic:IP               0           0  unlimited           0 admin
CP-Traffic:ARP              0           0  unlimited           0 admin
CP-Traffic:Fixup            0           0  unlimited           0 admin
CP-Traffic:NPCP             0           0  unlimited           0 admin
CP-Traffic:Unknown          0           0  unlimited           0 admin
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
clear resource usage	リソース使用状況の統計情報をクリアします。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスのリソース制限を設定します。
show resource types	リソース タイプのリストを表示します。

show rip database

RIP トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show rip database** コマンドを使用します。

show rip database [*ip_addr* [*mask*]]

構文の説明

ip_addr	（任意）指定したネットワーク アドレスの表示ルートを制限します。
mask	（任意）オプションのネットワーク アドレスのネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP ルーティング関連の **show** コマンドは、セキュリティ アプライアンスの特権モードで使用できます。RIP 関連の **show** コマンドを使用する場合に RIP コンフィギュレーション モードである必要はありません。

RIP データベースには RIP を通じて学習されたルートがすべて含まれます。このデータベースに表示されるルートはルーティング テーブルには必ずしも表示されません。ルーティング テーブルにルーティング プロトコル データベースから値を挿入する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次に、**show rip database** コマンドの出力例を示します。

```
hostname# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

次に、ネットワーク アドレスとマスクを指定した、**show rip database** コマンドの出力例を示します。

```
Router# show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

関連コマンド

コマンド	説明
router rip	RIP ルーティングをイネーブルにし、グローバル RIP ルーティング パラメータを設定します。

show route

ルーティング テーブルを表示するには、特権 EXEC モードで **show route** コマンドを使用します。

show route [*interface_name* [*ip_address* [*netmask* [**static**]]]]

構文の説明

static	（任意）表示対象をスタティック ルートに限定します。
interface_name	（任意）表示対象を指定のインターフェイスを使用するルート エントリに限定します。
ip_address	（任意）表示対象を指定の宛先へのルートに限定します。
netmask	（任意）*ip_address* に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show route** コマンドの出力例を示します。

```
hostname# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

次に、ASA5505 適応型セキュリティ アプライアンスの show route コマンドの出力例を示します。この例には、個々のユーザ認証用に VPN ハードウェア クライアントが使用する内部ループバック アドレスが表示されます。

```
hostname(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	スタティックまたはデフォルト ルートを作成します。
show running-config route	実行コンフィギュレーションの route コマンドを表示します。

CHAPTER 28

show running-config コマンド～ show running-config isakmp コマンド

show running-config

セキュリティ アプライアンス上で現在実行されているコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**all**] [*command*]

構文の説明

all	デフォルトを含め、動作設定全体を表示します。
command	特定のコマンドに関連付けられたコンフィギュレーションを表示します。

デフォルト

引数もキーワードも指定しない場合は、デフォルト以外に設定されているセキュリティ アプライアンス コンフィギュレーション全体が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドが変更されました。

使用上のガイドライン

show running-config コマンドは、セキュリティ アプライアンスのメモリにあるアクティブなコンフィギュレーション（保存されたコンフィギュレーションの変更を含む）を表示します。

show running-config コマンドでは **running-config** キーワードだけを使用できます。このキーワードは **no** または **clear** と一緒には使用できません。また、スタンドアロン コマンドとして使用することもできません。CLI では、サポートされていないコマンドとして処理されます。また、**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

セキュリティ アプライアンスのフラッシュ メモリに保存されたコンフィギュレーションを表示するには、**show configuration** コマンドを使用します。

（注） このコマンドを使用してセキュリティ アプライアンスへの接続または設定を行った後は、コンフィギュレーションに ASDM コマンドが表示されます。

例

次の例は、セキュリティ アプライアンス上で実行されているアクティブ コンフィギュレーションを表示する方法を示しています。

```
hostname# show running-config
: Saved
:
XXX Version X.X(X)
```

```
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
```

```
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

関連コマンド

コマンド	説明
configure	ターミナルからセキュリティ アプライアンスを設定します。

show running-config aaa

実行コンフィギュレーションの AAA コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa** コマンドを使用します。

show running-config aaa [accounting | authentication | authorization | mac-exempt | proxy-limit]

構文の説明

accounting	（任意）アカウンティング関連の AAA コンフィギュレーションを表示します。
authentication	（任意）認証関連の AAA コンフィギュレーションを表示します。
authorization	（任意）認可関連の AAA コンフィギュレーションを表示します。
mac-exempt	（任意）MAC アドレス免除の AAA コンフィギュレーションを表示します。
proxy-limit	（任意）ユーザ 1 人あたりに許可されている同時プロキシ接続数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config aaa** コマンドの出力例を示します。

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
hostname#
```

関連コマンド

コマンド	説明
aaa authentication match	アクセス リストで指定されるトラフィックの認証をイネーブルにします。
aaa authorization match	アクセス リストで指定されるトラフィックの認可をイネーブルにします。

コマンド	説明
aaa accounting match	アクセス リストで指定されるトラフィックのアカウンティングをイネーブルにします。
aaa max-exempt	認証と認可を免除される MAC アドレスの事前定義済みリストの使用を指定します。
aaa proxy-limit	ユーザ 1 人あたりに許可される同時プロキシ接続の最大数を設定して、uauth セッション制限を設定します。

show running-config aaa-server

AAA サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show running-config [**all**] **aaa-server** [*server-tag*] [**(***interface-name***)**] [**host** *hostname*]

構文の説明

all	（任意）デフォルトのコンフィギュレーション値など、実行コンフィギュレーションを表示します。
host *hostname*	（任意）AAA サーバの統計情報を表示する特定ホストのシンボリック名または IP アドレス。
(interface-name)	（任意）AAA サーバが配置されているネットワーク インターフェイス。
server-tag	（任意）サーバ グループのシンボリック名。

デフォルト

server-tag 値を省略すると、すべての AAA サーバのコンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、CLI ガイドラインに準拠するように変更されました。

使用上のガイドライン

このコマンドを使用して、特定のサーバ グループの設定を表示します。明示的に設定されている値に加えてデフォルト値も表示するには、**all** パラメータを使用します。

例

デフォルト AAA サーバ グループの実行コンフィギュレーションを表示するには、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
hostname(config)#
```

関連コマンド

コマンド	説明
show aaa-server	AAA サーバの統計情報を表示します。
clear configure aaa-server	AAA サーバ コンフィギュレーションをクリアします。

show running-config aaa-server host

特定サーバの AAA サーバ統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

構文の説明

all	（任意）デフォルトのコンフィギュレーション値など、実行コンフィギュレーションを表示します。
server-tag	サーバ グループのシンボリック名。

デフォルト

デフォルトのキーワードを省略すると、明示的に設定されているコンフィギュレーション値だけが表示され、デフォルト値は表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドを使用して、特定のサーバ グループの統計情報を表示します。デフォルトおよび明示的に設定された値を表示する場合は、デフォルトのパラメータを使用します。

例

サーバ グループ svrgrp1 の実行コンフィギュレーションを表示する場合は、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server svrgrp1
```

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバ、グループ、またはプロトコルの AAA サーバ設定を表示します。
clear configure aaa	すべてのグループのすべての AAA サーバの設定を削除します。

show running-config access-group

アクセス グループ情報を表示するには、特権 EXEC モードで **show running-config access-group** コマンドを使用します。

show running-config access-group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show running-config access-group** コマンドの出力例を示します。

```
hostname# show running-config access-group
access-group 100 in interface outside
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。

show running-config access-list

セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config access-list** コマンドを使用します。

show running-config [**default**] **access-list** [**alert-interval** | **deny-flow-max**]

show running-config [**default**] **access-list** *id* [*saddr_ip*]

構文の説明

alert-interval	syslog メッセージ 106001 を生成するアラートの間隔を表示します。このメッセージは、システムが拒否フローの最大数に達したことを警告するメッセージです。
deny-flow-max	作成できる同時拒否フローの最大数を表示します。
id	表示するアクセス リストを指定します。
saddr_ip	指定した送信元 IP アドレスを含むアクセス リスト要素を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

使用上のガイドライン

show running-config access-list コマンドを使用すると、セキュリティ アプライアンスで現在実行されているアクセス リスト コンフィギュレーションを表示できます。

例

次に、**show running-config access-list** コマンドの出力例を示します。

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

関連コマンド

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。

show running-config alias

コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示するには、特権 EXEC モードで **show running-config alias** コマンドを使用します。

show running-config alias {*interface_name*}

構文の説明

interface_name	destination_ip が上書きする内部ネットワーク インターフェイス名。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、エイリアス情報を表示する例を示します。

```
hostname# show running-config alias
```

関連コマンド

コマンド	説明
alias	エイリアスを作成します。
clear configure alias	エイリアスを削除します。

show running-config arp

arp コマンドによって作成された、実行コンフィギュレーションのスタティック ARP エントリを表示するには、特権 EXEC モードで **show running-config arp** コマンドを使用します。

show running-config arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config arp** コマンドの出力例を示します。

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show running-config arp timeout

実行コンフィギュレーションの ARP タイムアウト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp timeout** コマンドを使用します。

show running-config arp timeout

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show arp timeout** から変更されました。

例

次に、**show running-config arp timeout** コマンドの出力例を示します。

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。

show running-config arp-inspection

実行コンフィギュレーションの ARP インスペクション コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp-inspection** コマンドを使用します。

show running-config arp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show arp timeout** から変更されました。

例

次に、**show running-config arp-inspection** コマンドの出力例を示します。

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear configure arp-inspection	ARP インスペクション コンフィギュレーションをクリアします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。

show running-config asdm

実行コンフィギュレーションの **asdm** コマンドを表示するには、特権 EXEC モードで **show running-config asdm** コマンドを使用します。

show running-config asdm [**group** | **location**]

構文の説明

group	（任意）表示を、実行コンフィギュレーションの **asdm group** コマンドに制限します。
location	（任意）表示を、実行コンフィギュレーションの **asdm location** コマンドに制限します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show running-config pdm** コマンドから **show running-config asdm** コマンドに変更されました。

使用上のガイドライン

asdm コマンドをコンフィギュレーションから削除するには、**clear configure asdm** コマンドを使用します。

（注） マルチ コンテキスト モードで動作しているセキュリティ アプライアンスでは、**show running-config asdm group** コマンドおよび **show running-config asdm location** コマンドは、システム実行スペースのみで使用できます。

例

次に、**show running-configuration asdm** コマンドの出力例を示します。

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。

show running-config auth-prompt

現在の認証プロンプト チャレンジ テキストを表示するには、グローバル コンフィギュレーション モードで show running-config auth-prompt コマンドを使用します。

show running-config [default] auth-prompt

構文の説明

default	（任意）デフォルトの認証プロンプト チャレンジ テキストを表示します。

デフォルト

設定されている認証プロンプト チャレンジ テキストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

auth-prompt コマンドを使用して認証プロンプトを設定した後に **show running-config auth-prompt** コマンドを使用すると、現在のプロンプト テキストが表示されます。

例

次に、**show running-config auth-prompt** コマンドの出力例を示します。

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
hostname(config)#
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
clear configure auth-prompt	ユーザ認可プロンプトをデフォルト値にリセットします。

show running-config banner

指定したバナー、およびそのバナーに設定されているすべての行を表示するには、特権 EXEC モードで **show running-config banner** コマンドを使用します。

show running-config banner [**exec** | **login** | **motd**]

構文の説明

exec	（任意）イネーブル プロンプトの前にバナーを表示します。
login	（任意）Telnet を使用してセキュリティ アプライアンスにアクセスした場合に、パスワード ログイン プロンプトの前にバナーを表示します。
motd	（任意）Message-of-The-Day バナーを表示します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**running-config** キーワードが追加されました。

使用上のガイドライン

show running-config banner コマンドは、指定したバナー キーワード、およびそのバナーに設定されているすべての行を表示します。キーワードが指定されていない場合は、すべてのバナーが表示されます。

例

次に、Message-of-The-Day（motd）バナーを表示する例を示します。

```
hostname# show running-config banner motd
```

関連コマンド

コマンド	説明
banner	バナーを作成します。
clear configure banner	バナーを削除します。

show running-config class

リソース クラス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config class** コマンドを使用します。

show running-config class

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config class** コマンドの出力例を示します。

```
hostname# show running-config class

class default
  limit-resource All 0
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。

show running-config class-map

クラス マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config class-map** コマンドを使用します。

show running-config [**all**] **class-map** [*class_map_name* | **type** {**management** | **regex** | **inspect** [*protocol*]}]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべてのコマンドを表示します。
class_map_name	（任意）クラス マップ名の実行コンフィギュレーションを表示します。
inspect	（任意）インスペクション クラス マップを表示します。
management	（任意）管理クラス マップを表示します。
protocol	（任意）表示するアプリケーション マップのタイプを指定します。利用可能なタイプは次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	（任意）正規表現クラス マップを表示します。
type	（任意）表示するクラス マップのタイプを指定します。レイヤ 3/4 クラス マップを表示する場合は、タイプを指定しないでください。

デフォルト

match any コマンドを 1 つだけ含む **class-map class-default** コマンドが、デフォルトのクラス マップです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

例

次に、**show running-config class-map** コマンドの出力例を示します。

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
hostname#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。

show running-config client-update

グローバル クライアント更新コンフィギュレーション情報を表示するには、グローバル コンフィギュレーション モードまたはトンネル グループ IPSec 属性コンフィギュレーション モードで、**show running-config client-update** コマンドを使用します。

show running-config client-update

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。

使用上のガイドライン

このコマンドを使用して、グローバル クライアント更新コンフィギュレーション情報を表示します。

例

次に、グローバル コンフィギュレーション モードでの **show running-config client-update** コマンド、およびクライアント更新がイネーブルなコンフィギュレーションでのコマンドの出力例を示します。

```
hostname(config)# show running-config client-update
hostname(config)# client-update enable
```

関連コマンド

コマンド	説明
clear configure client-update	クライアントアップデート コンフィギュレーション全体をクリアします。
client-update	クライアント アップデートを設定します。

show running-config clock

実行コンフィギュレーションのクロック コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config clock** コマンドを使用します。

show running-config [**all**] **clock**

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての **clock** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オフセットを設定しなかった場合は、**all** キーワードを指定すると、**clock summer-time** コマンドの正確な日時とともにオフセットのデフォルト設定も表示されます。

例

次に、**show running-config clock** コマンドの出力例を示します。**clock summer-time** コマンドのみが設定されています。

```
hostname# show running-config clock
clock summer-time EDT recurring
```

次に、**show running-config all clock** コマンドの出力例を示します。設定されていない **clock timezone** コマンドのデフォルト設定および **clock summer-time** コマンドの詳細な情報が表示されています。

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。

show running-config command-alias

設定されているコマンド エイリアスを表示するには、特権 EXEC モードで **show running-config command-alias** コマンドを表示します。

show running-config [**all**] **command-alias**

構文の説明

all	（任意）デフォルトを含め、設定されているすべてのコマンド エイリアスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

all キーワードを入力しない場合は、デフォルト以外のコマンド エイリアスのみが表示されます。

例

次の例では、デフォルト値を*含めて*、セキュリティ アプライアンスで設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

次の例では、デフォルト値を*除いて*、セキュリティ アプライアンスで設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
clear configure command-alias	デフォルト以外のすべてのコマンド エイリアスを削除します。

show running-config compression

実行コンフィギュレーションの圧縮コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config compression** コマンドを使用します。

show running-config compression

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、実行コンフィギュレーション内の圧縮コンフィギュレーションを表示する例を示します。

```
hostname# show running-config compression
compression svc http-comp
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、およびポート転送接続に対して圧縮をイネーブルにします。

show running-config console timeout

コンソール接続のタイムアウト値を表示するには、特権 EXEC モードで **show running-config console timeout** コマンドを使用します。

show running-config console timeout

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、コンソール接続のタイムアウト設定を表示する方法を示しています。

```
hostname# show running-config console timeout
console timeout 0
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
clear configure console	コンソール接続の設定をデフォルトにリセットします。

show running-config context

システム実行スペースのコンテキスト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config context** コマンドを使用します。

show running-config [**all**] **context**

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべてのコマンドを表示します。**mac-address auto** コマンドを使用する場合、**all** キーワードを使用すると、割り当てられているすべての MAC アドレスを表示できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(5)	**all** キーワードを使用すると、**mac-address auto** コマンドを設定するときに、共有インターフェイスに割り当てられている MAC アドレスを表示できます。

使用上のガイドライン

mac-address auto コマンドを使用して共有インターフェイスの一意な MAC アドレスを生成する場合、割り当てられている MAC アドレスを表示するには **all** オプションが必要です。**mac-address auto** コマンドは、ユーザがグローバル コンフィギュレーション モードだけで設定可能ですが、**mac-address auto** コマンドは、各コンテキストのコンフィギュレーションで、割り当てられている MAC アドレスとともに読み取り専用エントリとして表示されます。コンテキスト内で **nameif** コマンドで設定される共有インターフェイスだけに MAC アドレスが割り当てられます。

（注） MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
hostname# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。

コマンド	説明
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
mac-address auto	共有インターフェイスの一意の MAC アドレスを自動的に生成します。

show running-config crypto

IPSec、クリプト マップ、ダイナミック クリプト マップ、および ISAKMP を含めた暗号コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto** コマンドを使用します。

show running-config crypto

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

特権 EXEC モードで入力した次の例では、すべての暗号コンフィギュレーション情報を表示しています。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto dynamic-map

ダイナミック クリプト マップを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto dynamic-map** コマンドを使用します。

show running-config crypto dynamic-map

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、ダイナミック クリプト マップに関するすべてのコンフィギュレーション情報を表示する例を示します。

```
hostname(config)# show running-config crypto dynamic-map

Crypto Map Template "dyn1" 10

        access-list 152 permit ip host 172.21.114.67 any
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={ tauth, t1, }
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto ipsec

完全な IPSec コンフィギュレーションを表示するには、グローバル コンフィギュレーションまたは特権 EXEC モードで **show running-config crypto ipsec** コマンドを使用します。

show running-config crypto ipsec

構文の説明

このコマンドにデフォルトの動作または値はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、IPSec コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto isakmp** コマンドを使用します。

show running-config crypto isakmp

構文の説明

このコマンドにデフォルトの動作または値はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show running-config isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show running-config crypto isakmp** コマンドが代わりに使用されます。

例

グローバル コンフィギュレーション モードで発行した次の例では、ISKAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config crypto isakmp
crypto isakmp enable inside
crypto isakmp policy 1 authentication pre-share
crypto isakmp policy 1 encryption 3des
crypto isakmp policy 1 hash md5
crypto isakmp policy 1 group 2
crypto isakmp policy 1 lifetime 86400
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show crypto isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto map

すべてのクリプト マップのすべてのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto map** コマンドを使用します。

show running-config crypto map

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、特権 EXEC モードでコマンドを入力し、すべてのクリプト マップのすべてのコンフィギュレーション情報を表示する例を示します。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config ctl-file

設定されている CTL ファイルのインスタンスを表示するには、特権 EXEC モードで **show running-config ctl-file** コマンドを使用します。

show running-config [**all**] **ctl-file** [*ctl_name*]

構文の説明

ctl_name	（任意）CTL ファイル インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**show running-config ctl-file** コマンドを使用して、設定されている CTL ファイル インスタンスを表示する例を示します。

```
hostname# show running-config all ctl-file asa_ctl
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（**Phone-Proxy**）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

show running-config ctl-provider

現在実行されているすべての証明書信頼リスト プロバイダーのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ctl-provider** コマンドを使用します。

show running-config [**all**] **ctl-provider** [*provider_name*]

構文の説明

all	デフォルトから変更していないコマンドを含め、すべての TLS プロキシ コマンドを表示します。
provider_name	表示する CTL プロバイダーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**show running-config ctl-provider** コマンドの出力例を示します。

```
hostname# show running-config ctl-provider
ctl-provider ctl_prov
    client interface inside address 195.168.2.103
    client username CCMAdministrator password xxxxxxxxxxxx encrypted
    export certificate local_ccm
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。

show running-config ddns

実行コンフィギュレーションの DDNS 更新方式を表示するには、特権 EXEC モードで **show running-config ddns** コマンドを使用します。

show running-config [**all**] **ddns** [**update**]

構文の説明

all	（任意）デフォルトのコンフィギュレーション値など、実行コンフィギュレーションを表示します。
update	（任意）DDNS 更新方式情報の表示を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、実行コンフィギュレーションで名前に test が含まれる DDNS 方式を表示する例を示します。

```
hostname# show running-config all ddns | grep test
ddns update method test
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。
show ddns update method	設定済みの DDNS 方式ごとにタイプと間隔を表示します。DDNS アップデートを実行する DHCP サーバ。

show running-config dhcp-client

実行コンフィギュレーションの DHCP クライアント更新パラメータを表示するには、特権 EXEC モードで **show running-config dhcp-client** コマンドを使用します。

show running-config [**all**] **dhcp-client**

構文の説明

all	（任意）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、A および PTR の両方のレコードの更新を指定する、実行コンフィギュレーションの DHCP クライアント更新パラメータを表示する例を示します。

```
hostname# show running-config all dhcp-client | grep both
dhcp-client update dns server both
```

関連コマンド

コマンド	説明
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
clear configure dhcp-client	DHCP クライアント コンフィギュレーションをクリアします。

show running-config dhcpd

DHCP コンフィギュレーションを表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show running-config dhcpd** コマンドを使用します。

show running-config dhcpd

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show dhcpd** コマンドから **show running-config dhcpd** コマンドに変更されました。

使用上のガイドライン

show running-config dhcpd コマンドは、実行コンフィギュレーションで入力された DHCP コマンドを表示します。DHCP のバインディング、状態、および統計情報を表示するには、**show dhcpd** コマンドを使用します。

例

次に、**show running-config dhcpd** コマンドの出力例を示します。

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
debug dhcpd	DHCP サーバのデバッグ情報を表示します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

show running-config dhcprelay

現在の DHCP リレー エージェント コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dhcprelay** コマンドを使用します。

show running-config dhcprelay

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show running-config dhcprelay コマンドは、現在の DHCP リレー エージェント コンフィギュレーションを表示します。DHCP リレー エージェントのパケット統計情報を表示するには、**show dhcprelay statistics** コマンドを使用します。

例

次に、**show running-config dhcprelay** コマンドの出力例を示します。

```
hostname(config)# show running-config dhcprelay

dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェントの統計カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。

show running-config dns

実行コンフィギュレーションの DNS コンフィギュレーションを表示するには、**show running-config dns** コマンドを特権 EXEC モードで使用します。

show running-config dns

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、**show running-config dns** コマンドの出力例を示します。

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

show running-config dns server-group

実行コンフィギュレーションの DNS コンフィギュレーションを表示するには、**show running-config dns** コマンドを特権 EXEC モードで使用します。

show [**all**] **running-config dns server-group** [*name*]

構文の説明

all	1 つまたはすべての DNS サーバ グループについて、デフォルトおよび明示的に設定されたコンフィギュレーション情報を表示します。
name	コンフィギュレーション情報を表示する DNS サーバ グループの名前を指定します。

デフォルト

DNS サーバ グループ名を省略すると、既存の DNS サーバ グループ コンフィギュレーションがすべて表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1 (1)	このコマンドが導入されました。

例

次に、**show running-config dns server-group** コマンドの出力例を示します。

```
hostname# show running-config dns server-group
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 90.1.1.22
 domain-name frqa.cisco.com
dns server-group writers1
 retries 10
 timeout 3
 name-server 10.86.194.61
 domain-name doc-group
hostname#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。

show running-config domain-name

実行コンフィギュレーションのドメイン名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config domain-name** コマンドを使用します。

show running-config domain-name

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show domain-name** から変更されました。

例

次に、**show running-config domain-name** コマンドの出力例を示します。

```
hostname# show running-config domain-name
example.com
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。

show running-config dynamic-access-policy-record

すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dynamic-access-policy-record** コマンドを使用します。

show running-config dynamic-access-policy-record [*name***]**

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

デフォルト

すべての属性が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**show running-config dynamic-access-policy-record** コマンドを使用して、Finance という名前の DAP レコードの統計情報を表示する例を示します。

```
ASA(config)#show running-config dynamic-access-policy-record Finance
dynamic-access-policy-record Finance
description value “Finance users from trusted device”
network-acl FinanceFirewallAcl
user-message “Limit access to the Finance network”
priority 2
webvpn
  appl-acl FinanceWebvpnAcl
  url-list value FinanceLinks,StockLinks
  port-forward enable FinanceApps
  file-browsing enable
  file-entry enablehostname#
```

関連コマンド

コマンド	説明
clear config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定された DAP レコードを削除します。
dynamic-access-policy-record	DAP レコードを作成します。

show running-config enable

暗号化されたイネーブル パスワードを表示するには、特権 EXEC モードで **show running-config enable** コマンドを使用します。

show running-config enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show enable** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは **encrypted** キーワードとともに表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config enable** コマンドの出力例を示します。

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

関連コマンド

コマンド	説明
disable	特権 EXEC モードを終了します。
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。

show running-config established

確立されている接続に基づく、許可済みの着信接続を表示するには、特権 EXEC モードで **show running-config established** コマンドを使用します。

show running-config established

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** が追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインがありません。

例

次に、確立されている接続に基づいて着信接続を表示する例を示します。

```
hostname# show running-config established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
clear configure established	確立されたコマンドをすべて削除します。

show running-config failover

コンフィギュレーション内の **failover** コマンドを表示するには、特権 EXEC モードで **show running-config failover** コマンドを使用します。

show running-config [**all**] **failover**

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての failover コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config failover コマンドは、実行コンフィギュレーションに含まれる **failover** コマンドを表示します。**monitor-interface** コマンドまたは **join-failover-group** コマンドは表示されません。

例

次に、フェールオーバーを設定する前のデフォルト フェールオーバー コンフィギュレーションの例を示します。

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
```

関連コマンド

コマンド	説明
show failover	フェールオーバーの状態および統計情報を表示します。

show running-config filter

フィルタリング コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config filter** コマンドを使用します。

show running-config filter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show running-config filter コマンドは、セキュリティ アプライアンスのフィルタリング コンフィギュレーションを表示します。

例

次に、**show running-config filter** コマンドの出力例を示します。セキュリティ アプライアンスのフィルタリング コンフィギュレーションが表示されています。

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

この例では、アドレス 10.86.194.170 のポート 80 で ActiveX フィルタリングがイネーブルになっています。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。

show running-config fips

セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示するには、**show running-config fips** コマンドを使用します。

show running-config fips

構文の説明

fips	FIPS-2 準拠情報

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

show running-config fips コマンドを使用すると、現在実行されている FIPS コンフィギュレーションを表示できます。**running-config** キーワードは、**show running-config fips** コマンド内だけで使用します。このキーワードを no または clear とともに使用することや、スタンドアロン コマンドとして使用することはサポートされていません。また、**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

例

```
hostname(config)# show running-config fips
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。

show running-config fragment

フラグメント データベースの現在のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config fragment** コマンドを使用します。

show running-config fragment [*interface*]

構文の説明

interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config fragment コマンドは、フラグメント データベースの現在のコンフィギュレーションを表示します。インターフェイス名を指定した場合は、指定したインターフェイスに存在するデータベースの情報だけが表示されます。インターフェイス名を指定しなかった場合、このコマンドはすべてのインターフェイスに適用されます。

show running-config fragment コマンドを使用すると、次の情報が表示されます。

- Size : **size** キーワードで設定されるパケットの最大数。この値は、インターフェイスで許容されるフラグメントの最大数です。
- Chain : **chain** キーワードで設定される、単一パケットのフラグメントの最大数。
- Timeout : **timeout** キーワードで設定される最大秒数。これは、フラグメント化されたパケット全体が到着するのを待機する最大秒数です。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

例

次に、すべてのインターフェイスのフラグメント データベースの状態を表示する例を示します。

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

```
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次に、名前が「outside」で始まるインターフェイスのフラグメント データベースの状態を表示する例を示します。

（注） この例では、「outside1」、「outside2」および「outside3」という名前のインターフェイスが表示されます。

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次に、「outside1」という名前のインターフェイスについてのみ、フラグメント データベースの状態を表示する例を示します。

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。

show running-config ftp mode

FTP に設定されているクライアント モードを表示するには、特権 EXEC モードで **show running-config ftp mode** コマンドを使用します。

show running-config ftp mode

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show running-config ftp mode コマンドは、セキュリティ アプライアンスが FTP サーバにアクセスするときに使用するクライアント モードを表示します。

例

次に、**show running-config ftp-mode** コマンドの出力例を示します。

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

関連コマンド

コマンド	説明
copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
ftp mode passive	セキュリティ アプライアンスが FTP サーバにアクセスするときに使用する FTP クライアント モードを設定します。

show running-config global

コンフィギュレーション内の **global** コマンドを表示するには、特権 EXEC モードで **show running-config global** コマンドを使用します。

show running-config global

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

例

次に、**show running-config global** コマンドの出力例を示します。

```
hostname# show running-config global
global (outside1) 10 interface
```

関連コマンド

コマンド	説明
clear configure global	コンフィギュレーションから **global** コマンドを削除します。
global	グローバル アドレスのプールからエントリを作成します。

show running-config group-delimiter

トンネルのネゴシエート時に受信したユーザ名からグループ名を解析するときに使用する、現在のデリミタを表示するには、グローバル コンフィギュレーション モードまたはトンネル グループ IPSec 属性コンフィギュレーション モードで **show running-config group-delimiter** コマンドを使用します。

show running-config group-delimiter

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。

使用上のガイドライン

このコマンドを使用して、現在設定されている group-delimiter を表示します。

例

次に、**show running-config group-delimiter** コマンドおよびその出力例を示します。

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

関連コマンド

コマンド	説明
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。

show running-config group-policy

特定のグループ ポリシーの実行コンフィギュレーションを表示するには、特権 EXEC モードでグループ ポリシーの名前を指定して **show running-config group-policy** コマンドを使用します。すべてのグループ ポリシーの実行コンフィギュレーションを表示するには、特定のグループ ポリシーを指定しないでこのコマンドを使用します。表示にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] group-policy [*name***]**

構文の説明

all	（任意）実行コンフィギュレーションを、デフォルト値を含めて表示します。
name	（任意）グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーの実行コンフィギュレーションを、デフォルト値を含めて表示する例を示します。

```
hostname# show running-config all group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成、編集、または削除します。

コマンド	説明
group-policy attributes	グループ ポリシー属性モードを開始します。このモードでは、指定したグループ ポリシーの AVP を設定できます。
clear config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。

show running-config http

現在の設定済み HTTP コマンドのセットを表示するには、特権 EXEC モードで **show running-config http** コマンドを使用します。

show running-config http

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config http** コマンドの出力例を示します。

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

関連コマンド

コマンド	説明
clear http	HTTP コンフィギュレーションを削除します。HTTP サーバがディセーブルになり、HTTP サーバにアクセスできるホストが削除されます。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由するセキュリティ アプライアンスのインターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザの証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバをイネーブルにします。

show running-config icmp

ICMP トラフィックに設定されているアクセス ルールを表示するには、特権 EXEC モードで **show running-config icmp** コマンドを使用します。

show running-config icmp *map_name*

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show running-config icmp コマンドは、ICMP トラフィックに設定されているアクセス ルールを表示します。

例

次に、**show running-config icmp** コマンドの出力例を示します。

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show running-config imap4s

IMAP4S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config imap4s** コマンドを使用します。

show running-config [all] imap4s

構文の説明

all	（任意）実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
webvpn	•	—	•	—	—

例

次に、**show running-config imap4s** コマンドの出力例を示します。

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
imap4s	IMAP4S 電子メール プロキシ コンフィギュレーションを作成または編集します。

show running-config interface

実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config interface** コマンドを使用します。

show running-config [**all**] **interface** [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての **interface** コマンドを表示します。
interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しなかった場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。

例

次に、**show running-config interface** コマンドの出力例を示します。この例では、すべてのインターフェイスの実行コンフィギュレーションが表示されています。GigabitEthernet0/2 インターフェイスおよび GigabitEthernet0/3 インターフェイスは未設定のため、デフォルトのコンフィギュレーションが表示されています。Management0/0 インターフェイスにもデフォルトの設定が表示されています。

```
hostname# show running-config interface
!
```

```
interface GigabitEthernet0/0
 no shutdown
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 no shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/1.1
 vlan 101
 no shutdown
 nameif dmz
 security-level 50
 ip address 10.50.1.1 255.255.255.0
 mac-address 000C.F142.4CDE standby 020C.F142.4CDE
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 security-level 0
 no ip address
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show running-config ip address

実行コンフィギュレーションの IP アドレス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip address** コマンドを使用します。

show running-config ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しなかった場合は、すべてのインターフェイスの IP アドレス コンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内だけで指定できます。

このコマンドは、管理 IP アドレスだけを表示するコマンドであるため、トランスペアレント ファイアウォール モードにおいてはインターフェイスを指定しないでください。トランスペアレント ファイアウォールでは、インターフェイスに IP アドレスが関連付けられていません。

この表示には、**nameif** コマンドおよび **security-level** コマンドのコンフィギュレーションも表示されます。

例

次に、**show running-config ip address** コマンドの出力例を示します。

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
```

```
 security-level 100
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイア ウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config ip audit attack

実行コンフィギュレーションの **ip audit attack** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit attack** コマンドを使用します。

show running-config ip audit attack

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip audit attack** から変更されました。

例

次に、**show running-config ip audit attack** コマンドの出力例を示します。

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit info

実行コンフィギュレーションの **ip audit info** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit info** コマンドを使用します。

show running-config ip audit info

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip audit info** から変更されました。

例

次に、**show running-config ip audit info** コマンドの出力例を示します。

```
hostname# show running-config ip audit info
ip audit info action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit interface

実行コンフィギュレーションの **ip audit interface** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit interface** コマンドを使用します。

show running-config ip audit interface [*interface_name*]

構文の説明

interface_name	（任意）インターフェイス名を指定します。

デフォルト

インターフェイス名を指定しなかった場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip audit interface** から変更されました。

例

次に、**show running-config ip audit interface** コマンドの出力例を示します。

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit name

実行コンフィギュレーションの **ip audit name** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit name** コマンドを使用します。

show running-config ip audit name [*name* [**info** | **attack**]]

構文の説明

attack	（任意）攻撃シグニチャに対する名前付き監査ポリシー コンフィギュレーションを表示します。
info	（任意）情報シグニチャに対する名前付き監査ポリシー コンフィギュレーションを表示します。
name	（任意）**ip audit name** コマンドを使用して作成した監査ポリシー名に関するコンフィギュレーションを表示します。

デフォルト

名前を指定しなかった場合は、すべての監査ポリシーのコンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip audit name** から変更されました。

例

次に、**show running-config ip audit name** コマンドの出力例を示します。

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit signature

実行コンフィギュレーションの **ip audit signature** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit signature** コマンドを使用します。

show running-config ip audit signature [*signature_number*]

構文の説明

signature_number	（任意）シグニチャ番号に対応するコンフィギュレーションを表示します（存在する場合）。サポートされているシグニチャのリストについては、**ip audit signature** コマンドを参照してください。

デフォルト

番号を指定しなかった場合は、すべてのシグニチャのコンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip audit signature** から変更されました。

例

次に、**show running-config ip audit signature** コマンドの出力例を示します。

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip local pool

IP アドレス プールを表示するには、特権 EXEC モードで **show running-config ip local pool** コマンドを使用します。

show running-config ip local pool [*poolname*]

構文の説明

poolname	（任意）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ip local pool** コマンドの出力例を示します。

```
hostname(config)# show running-config ip local pool firstpool

Pool            Begin           End             Mask            Free    In use
firstpool               10.20.30.40     10.20.30.50     255.255.255.0      11
    0
Available Addresses:
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

show running-config ip verify reverse-path

実行コンフィギュレーションの **ip verify reverse-path** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip verify reverse-path** コマンドを使用します。

show running-config ip verify reverse-path [interface *interface_name*]

構文の説明

interface *interface_name*	（任意）指定したインターフェイスのコンフィギュレーションを表示します。

デフォルト

このコマンドは、すべてのインターフェイスのコンフィギュレーションを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ip verify reverse-path** から変更されました。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
hostname# show running-config ip verify reverse-path
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。

show running-config ipv6

実行コンフィギュレーションの IPv6 コマンドを表示するには、特権 EXEC モードで **show running-config ipv6** コマンドを使用します。

show running-config [**all**] **ipv6**

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、実行コンフィギュレーションのすべての **ipv6** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ipv6** コマンドの出力例を示します。

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

関連コマンド

コマンド	説明
debug ipv6	IPv6 デバッグ メッセージを表示します。
show ipv6 access-list	IPv6 アクセス リストを表示します。
show ipv6 interface	IPv6 インターフェイスのステータスを表示します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

show running-config isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config isakmp** コマンドを使用します。

show running-config isakmp

構文の説明

このコマンドにデフォルトの動作または値はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show running-config isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show running-config crypto isakmp** コマンドが代わりに使用されます。

例

グローバル コンフィギュレーション モードで発行した次の例では、ISKAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

CHAPTER 29

show running-config ldap コマンド～ show running-config wccp コマンド

show running-config ldap

実行されている LDAP 属性マップ内にある LDAP 属性名と値のマッピングを表示するには、特権 EXEC モードで **show running-config ldap** コマンドを使用します。

show running-config [**all**] **ldap attribute-map** *name*

構文の説明

all	すべての LDAP 属性マップを表示します。
name	表示する個々の LDAP 属性マップを指定します。

デフォルト

デフォルトでは、すべての属性マップ、マッピング名、およびマッピング値が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、セキュリティ アプライアンス上で実行されている属性マップに含まれる LDAP 属性名と値のマッピングを表示します。すべての属性マップを表示するには、**all** オプションを使用します。また、単一の属性マップを表示するには、マップ名を指定します。**all** オプションと LDAP 属性マップ名をどちらも指定しなかった場合は、すべての属性マップ、マッピング名、および マッピング値が表示されます。

例

次に、特権 EXEC モードでコマンドを入力し、実行されている特定の属性マップ「myldapmap」の属性名と値のマッピングを表示する例を示します。

```
hostname# show running-config ldap attribute-map myldapmap
map-name Hours cVPN3000-Access-Hours
map-value Hours workDay Daytime
```

次に、実行されているすべての属性マップ内にある、すべての属性名と値のマッピングを表示するコマンドを示します。

```
hostname# show running-config all ldap attribute-map
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map（**AAA** サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

show running-config logging

現在実行されているすべてのロギング コンフィギュレーションを表示するには、特権 EXEC モードで **show runnig-config logging** コマンドを使用します。

show running-config [all] logging [level | disabled]

構文の説明

all	（任意）設定をデフォルトから変更していないコマンドを含めて、ロギング コンフィギュレーションを表示します。
disabled	（任意）ディセーブルにされたシステム ログ メッセージの設定だけを表示します。
level	（任意）デフォルト以外の重大度を持つシステム ログ メッセージの設定だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0 (1)	このコマンドは、**show logging** コマンドから変更されました。

例

次に、**show running-config logging disabled** コマンドの例を示します。

```
hostname# show running-config logging disabled

no logging message 720067
```

関連コマンド

コマンド	説明
logging message	ロギングを設定します。
show logging	ログ バッファおよびその他のロギング設定を表示します。

show running-config mac-address

実行コンフィギュレーションの **mac-address auto** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-address** コマンドを使用します。

show running-config mac-address

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config mac-address** コマンドの出力例を示します。

```
hostname# show running-config mac-address
no mac-address auto
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブとスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mac-address auto	マルチ コンテキスト モードでの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

show running-config mac-address-table

実行コンフィギュレーションの **mac-address-table static** および **mac-address-table aging-time** のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-address-table** コマンドを使用します。

show running-config mac-address-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-address-table
mac-address-table aging-time 50
mac-address-table static inside1 0010.7cbe.6101
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

show running-config mac-learn

実行コンフィギュレーションの **mac-learn** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-learn** コマンドを使用します。

show running-config mac-learn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-learn
mac-learn disable
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

show running-config mac-list

mac-list コマンドですでに指定されている MAC アドレスのリストを、MAC リスト番号を指定して表示するには、特権 EXEC モードで **show running-config mac-list** コマンドを使用します。

show running-config mac-list *id*

構文の説明

id	16 進数形式の MAC アドレス リスト番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

show running-config aaa コマンドは、AAA コンフィギュレーションに含まれる **mac-list** コマンド ステートメントを表示します。

例

次に、*id* が adc と等しい MAC アドレス リストを表示する例を示します。

```
hostname(config)# show running-config mac-list adc
mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
clear configure mac-list	指定した **mac-list** コマンド ステートメントを削除します。
show running-config aaa	実行 AAA コンフィギュレーション値を表示します。

show running-config management-access

管理アクセス用に設定されている内部インターフェイスの名前を表示するには、特権 EXEC モードで **show running-config management-access** コマンドを使用します。

show running-config management-access

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます （インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます)。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname# management-access inside
hostname# show running-config management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show running-config monitor-interface

実行コンフィギュレーションのすべての **monitor-interface** コマンドを表示するには、特権 EXEC モードで **show running-config monitor-interface** コマンドを使用します。

show running-config [all] monitor-interface

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての **monitor-interface** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

monitor-interface コマンドは、すべての物理インターフェイスにおいてデフォルトでイネーブルになっています。このデフォルトのコンフィギュレーションを表示するには、このコマンドで **all** キーワードを使用する必要があります。

例

次に、**show running-config monitor-interface** コマンドの出力例を示します。最初のコマンドは **all** キーワードを指定せずに入力されているため、モニタリングがイネーブルであるインターフェイスのみが出力に表示されています。2 番めのコマンドは **all** キーワードを指定して入力されているため、デフォルトの **monitor-interface** コンフィギュレーションも表示されています。

```
hostname# show running-config monitor-interface
no monitor-interface outside
hostname#
hostname# show running-config all monitor-interface
monitor-interface inside
no monitor-interface outside
hostname#
```

関連コマンド

コマンド	説明
monitor-interface	指定したインターフェイスでフェールオーバーを目的とするヘルス モニタリングをイネーブルにします。
clear configure monitor-interface	実行コンフィギュレーションの **no monitor-interface** コマンドを削除し、デフォルトのインターフェイス ヘルス モニタリング状態を復元します。

show running-config mroute

コンフィギュレーション内のスタティック マルチキャスト ルート テーブルを表示するには、特権 EXEC モードで **show running-config mroute** コマンドを使用します。

show running-config mroute [*dst* [*src*]]

構文の説明

dst	マルチキャスト グループのクラス D アドレス。
src	マルチキャスト送信元の IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

例

次に、**show running-config mroute** コマンドの出力例を示します。

```
hostname# show running-config mroute
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。

show running-config mtu

現在の最大伝送単位のブロック サイズを表示するには、特権 EXEC モードで **show running-config mtu** コマンドを使用します。

show running-config mtu [*interface_name*]

構文の説明

interface_name	（任意）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show running-config mtu** コマンドの出力例を示します。

```
hostname# show running-config mtu
mtu outside 1500
mtu inside 1500
mtu dmz 1500
hostname# show running-config mtu outside
mtu outside 1500
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送単位値をクリアします。
mtu	インターフェイスの最大伝送単位を指定します。

show running-config multicast-routing

実行コンフィギュレーションに **multicast-routing** コマンドが存在する場合に、このコマンドを表示するには、特権 EXEC モードで **show running-config multicast-routing** コマンドを使用します。

show running-config multicast-routing

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config multicast-routing コマンドは、実行コンフィギュレーションに含まれる **multicast-routing** コマンドを表示します。実行コンフィギュレーションから **multicast-routing** コマンドを削除するには、**clear configure multicast-routing** コマンドを入力します。

例

次に、**show running-config multicast-routing** コマンドの出力例を示します。

```
hostname# show running-config multicast-routing

multicast-routing
```

関連コマンド

コマンド	説明
clear configure multicast-routing	実行コンフィギュレーションから **multicast-routing** コマンドを削除します。
multicast-routing	セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。

show running-config nac-policy

セキュリティ アプライアンス上の NAC ポリシーごとのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config nac-policy** コマンドを使用します。

show running-config [all] nac-policy [*nac-policy-name***]**

構文の説明

all	デフォルト設定を含め、NAC ポリシーの動作設定全体を表示します。
nac-policy-name	セキュリティ アプライアンスのコンフィギュレーションに含まれる NAC ポリシーの名前。

デフォルト

nac-policy-name を指定しなかった場合は、デフォルトで NAC ポリシーごとの名前とコンフィギュレーションが CLI に表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、nacapp1 および nacapp2 という名前の NAC ポリシーのコンフィギュレーションを表示する例を示します。

```
hostname# show running-config nac-policy
nac-policy framework nac-framework
 default-acl acl-1
 reval-period 36000
 sq-period 300
 exempt-list os "Windows XP" filter acl-2
nac-policy nacapp1 nacapp
 auth-vlan 1
 cas 209.165.202.129
 cam outside 209.165.201.22 community secretword
timeout 10
hostname#
```

各 NAC ポリシーの先頭行は、ポリシーの名前とタイプを示しています。タイプは次のとおりです。

- `nacapp`：Cisco NAC アプライアンスを使用して、リモート ホストのネットワーク アクセス ポリシーを提供します。表 29-1 に、**show running-config nac-policy** コマンドの応答として表示される nacapp 属性の説明を示します。
- `nac-framework`：Cisco Access Control Server を使用して、リモート ホストのネットワーク アクセス ポリシーを提供します。表 29-2 に、**show running-config nac-policy** コマンドの応答として表示される nac-framework 属性の説明を示します。

表 29-1　nacapp ポリシーの show running-config nac-policy コマンドのフィールド

フィールド	説明
auth-vlan	ポスチャ検証が進行中の間、ユーザ アクセスを制限する認証 VLAN。セキュリティ アプライアンスは、トンネルの完了時に、セッションに割り当てられた vlan 属性に auth-vlan の値をコピーします。ポスチャ検証が正常に行われた後、セキュリティ アプライアンスは NAC アプライアンスから取得したアクセス VLAN の値で vlan 属性の値を上書きします。
cam	この行には次の値が表示されます。 • Clean Access Manager と通信するために使用するセキュリティ アプライアンスのインターフェイス。 • CAM の IP アドレスまたはホスト名。 • CAM の SNMP コミュニティ ストリング。
cas	Clean Access Server の IP アドレスまたはホスト名。
timeout	ユーザ セッションを認証 VLAN に割り当てておくことのできる最大時間（分）。

表 29-2　nac-framework ポリシーの show running-config nac-policy コマンドのフィールド

フィールド	説明
default-acl	ポスチャ検証前に適用される NAC デフォルト ACL。セキュリティ アプライアンスは、ポスチャ検証の後、リモート ホストの Access Control Server から取得した ACL でデフォルト ACL を置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。
reval-period	NAC フレームワーク セッションで正常に完了したポスチャ検証の間隔（秒）。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ検証と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔（秒）。
exempt-list	ポスチャ検証を免除されるオペレーティング システム名。リモート コンピュータのオペレーティング システムがこの名前に一致する場合は、トラフィックをフィルタリングするオプションの ACL も表示されます。
authentication-server-group	NAC ポスチャ検証に使用される認証サーバ グループの名前。

関連コマンド

nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
clear configure nac-policy	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーを実行コンフィギュレーションから削除します。
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	VLAN マッピング セッション データを含む、IPSec、Cisco AnyConnect、NAC の各セッションの数を表示します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

show running-config name

IP アドレスに関連付けられている（**name** コマンドで設定された）名前のリストを表示するには、特権 EXEC モードで **show running-config name** コマンドを使用します。

show running-config name

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IP アドレスに関連付けられている名前のリストを表示する例を示します。

```
hostname# show running-config name
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
name	名前を IP アドレスに関連付けます。

show running-config nameif

実行コンフィギュレーションのインターフェイス名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config nameif** コマンドを使用します。

show running-config nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

構文の説明

mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しなかった場合は、すべてのインターフェイスのインターフェイス名コンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show nameif** から変更されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内だけで指定できます。

このコマンドの表示には、**security-level** コマンドのコンフィギュレーションも表示されます。

例

次に、**show running-config nameif** コマンドの出力例を示します。

```
hostname# show running-config nameif
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
!
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config names

IP アドレスから名前への変換を表示するには、特権 EXEC モードで **show running-config names** コマンドを使用します。

show running-config names

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

names コマンドとともに使用します。

例

次に、IP アドレスから名前への変換を表示する例を示します。

```
hostname# show running-config names
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
name	名前を IP アドレスに関連付けます。
names	**name** コマンドで設定できる IP アドレスから名前への変換をイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前のリストを表示します。

show running-config nat

ネットワークに関連付けられているグローバル IP アドレスのプールを表示するには、特権 EXEC モードで **show running-config nat** コマンドを使用します。

show running-config nat [*interface_name*] [*nat_id*]

構文の説明

interface_name	（任意）ネットワーク インターフェイスの名前。
nat_id	（任意）ホスト グループまたはネットワークの ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

使用上のガイドライン

このコマンドは、UDP プロトコルの最大接続値を表示します。UPD 最大接続値が設定されていない場合、この値はデフォルトで常に 0 と表示され、値が適用されません。

（注） トランスペアレント モードで有効な NAT ID は 0 のみです。

例

次に、ネットワークに関連付けられているグローバル IP アドレスのプールを表示する例を示します。

```
hostname# show running-config nat
nat (inside) 1001 10.7.2.0 255.255.255.224 0 0
nat (inside) 1001 10.7.2.32 255.255.255.224 0 0
nat (inside) 1001 10.7.2.64 255.255.255.224 0 0
nat (inside) 1002 10.7.2.96 255.255.255.224 0 0
nat (inside) 1002 10.7.2.128 255.255.255.224 0 0
nat (inside) 1002 10.7.2.160 255.255.255.224 0 0
nat (inside) 1003 10.7.2.192 255.255.255.224 0 0
nat (inside) 1003 10.7.2.224 255.255.255.224 0 0
```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーションを削除します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show running-config nat-control

NAT コンフィギュレーション要件を表示するには、特権 EXEC モードで **show running-config nat-control** コマンドを使用します。

show running-config nat-control

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config nat-control** コマンドの出力例を示します。

```
hostname# show running-config nat-control
no nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
nat-control	NAT ルールを設定していない場合でも、内部ホストが外部ネットワークと通信できるようにします。

show running-config ntp

実行コンフィギュレーションの NTP コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ntp** コマンドを使用します。

show running-config ntp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ntp** コマンドの出力例を示します。

```
hostname# show running-config ntp
ntp authentication-key 1 md5 test2
ntp authentication-key 2 md5 test
ntp trusted-key 1
ntp trusted-key 2
ntp server 10.1.1.1 key 1
ntp server 10.2.1.1 key 2 prefer
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバによる認証用パケットで使用するための、セキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show running-config object-group

現在のオブジェクト グループを表示するには、特権 EXEC モードで **show running-config object-group** コマンドを使用します。

show running-config [**all**] **object-group** [**protocol** | **service** | **network** | **icmp-type** | **id** *obj_grp_id*]

構文の説明

icmp-type	（任意）ICMP タイプのオブジェクト グループを表示します。
id obj_grp_id	（任意）指定したオブジェクト グループを表示します。
network	（任意）ネットワーク オブジェクト グループを表示します。
protocol	（任意）プロトコル オブジェクト グループを表示します。
service	（任意）サービス オブジェクト グループを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show running-config object-group** コマンドの出力例を示します。

```
hostname# show running-config object-group
object-group protocol proto_grp_1
    protocol-object udp
    protocol-object tcp
object-group service eng_service tcp
    port-object eq smtp
    port-object eq telnet
object-group icmp-type icmp-allowed
    icmp-object echo
    icmp-object time-exceeded
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。

コマンド	説明
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。

show running-config passwd

暗号化されたログイン パスワードを表示するには、特権 EXEC モードで **show running-config passwd** コマンドを使用します。

show running-config {**passwd** | **password**}

構文の説明

passwd | **password**	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show passwd** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは **encrypted** キーワードとともに表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config passwd** コマンドの出力例を示します。

```
hostname# show running-config passwd
passwd 2AfK9Kjr3BE2/J2r encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードをクリアします。
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。

show running-config phone-proxy

電話プロキシ固有の情報を表示するには、特権 EXEC モードで **show running-config phone-proxy** コマンドを使用します。

show running-config [**all**] **phone-proxy** [*phone_proxy_name*]

構文の説明

phone_proxy_name	（任意）電話プロキシ インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、**show running-config phone-proxy** コマンドを使用して、電話プロキシ固有の情報を表示する例を示します。

```
hostname# show running-config all phone proxy asa_phone_proxy
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

show running-config pim

実行コンフィギュレーションの PIM コマンドを表示するには、特権 EXEC モードで **show running-config pim** コマンドを使用します。

show running-config pim

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config pim コマンドは、グローバル コンフィギュレーション モードで入力された **pim** コマンドを表示します。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドは表示しません。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドを表示するには、**show running-config interface** コマンドを入力します。

例

次に、**show running-config pim** コマンドの出力例を示します。

```
hostname# show running-config pim

pim old-register-checksum
pim spt-threshold infinity
```

関連コマンド

コマンド	説明
clear configure pim	実行コンフィギュレーションから **pim** コマンドを削除します。
show running-config interface	インターフェイス コンフィギュレーション モードで入力されたインターフェイス コンフィギュレーション コマンドを表示します。

show running-config policy-map

すべてのポリシー マップ コンフィギュレーションまたはデフォルトのポリシー マップ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config policy-map** コマンドを使用します。

show running-config [all] policy-map [*policy_map_name* | **type inspect** [*protocol*]]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべてのコマンドを表示します。
policy_map_name	（任意）ポリシー マップ名の実行コンフィギュレーションを表示します。
protocol	（任意）表示するインスペクション ポリシー マップのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**
type inspect	（任意）インスペクション ポリシー マップを表示します。

デフォルト

all キーワードを省略すると、明示的に設定されているポリシー マップ コンフィギュレーションだけが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

all キーワードを指定すると、明示的に設定したポリシー マップ コンフィギュレーションの他に、デフォルトのポリシー マップ コンフィギュレーションも表示されます。

例

次に、**show running-config policy-map** コマンドの出力例を示します。

```
hostname# show running-config policy-map
!
policy-map localmap1
    description this is a test.
    class firstclass
    priority
    ids promiscuous fail0close
    set connection random-seq# enable
    class class-default
!
```

関連コマンド

コマンド	説明
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
clear configure policy-map	ポリシー コンフィギュレーション全体を削除します。

show running-config pop3s

POP3S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config pop3s** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] pop3s

構文の説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
webvpn	•	—	•	—	—

例

次に、**show running-config pop3s** コマンドの出力例を示します。

```
hostname# show running-config pop3s

pop3s
 server 10.160.102.188
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all pop3s

pop3s
 port 995
 server 10.160.102.188
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
pop3s	POP3S 電子メール プロキシ コンフィギュレーションを作成または編集します。

show running-config prefix-list

実行コンフィギュレーションの **prefix-list** コマンドを表示するには、特権 EXEC モードで **show running-config prefix-list** コマンドを使用します。

show running-config prefix-list

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show prefix-list** コマンドから **show running-config prefix-list** コマンドに変更されました。

使用上のガイドライン

prefix-list description コマンドは、常に実行コンフィギュレーション内の関連する **prefix-list** コマンドの前に表示されます。コマンドを入力した順序は関係ありません。

例

次に、**show running-config prefix-list** コマンドの出力例を示します。

```
hostname# show running-config prefix-list

!
prefix-list abc description A sample prefix list
prefix-list abc seq 5 permit 192.168.0.0/8 le 24
prefix-list abc seq 10 deny 10.0.0.0/8 le 32
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドをクリアします。

show running-config priority-queue

インターフェイスのプライオリティ キュー コンフィギュレーションの詳細を表示するには、特権 EXEC モードで **show running-config priority-queue** コマンドを使用します。

show running-config priority-queue *interface-name*

構文の説明

interface-name	プライオリティ キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、test という名前のインターフェイスについて show running-config priority-queue コマンドを使用した場合のコマンドの出力例を示します。

```
hostname# show running-config priority-queue test
priority-queue test
  queue-limit   50
  tx-ring-limit 10
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスに設定されているプライオリティ キューの統計情報を表示します。

show running-config privilege

コマンドまたはコマンドのセットの特権を表示するには、特権 EXEC モードで **show running-config privilege** コマンドを使用します。

show running-config [all] privilege [**all** | **command** *command* | **level** *level*]

構文の説明

all	（任意）最初の引数：デフォルトの特権レベルを表示します。
all	（任意）2 番めの引数：すべてのコマンドの特権レベルを表示します。
command *command*	（任意）特定のコマンドの特権レベルを表示します。
level *level*	（任意）指定したレベルに設定されているコマンドを表示します。有効な値は、0 ～ 15 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

show running-config privilege コマンドを使用すると、現在の特権レベルが表示されます。

例

```
hostname(config)# show running-config privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
privilege	コマンドの特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

show running-config regex

regex コマンドを使用して設定したすべての正規表現を表示するには、特権 EXEC モードで **show running-config regex** コマンドを使用します。

show running-config regex

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config regex** コマンドの出力例を示します。すべての正規表現が表示されています。

```
hostname# show running-config regex
regex test "string"
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラス マップを作成します。
clear configure regex	すべての正規表現をクリアします。
regex	正規表現を作成します。
test regex	正規表現をテストします。

show running-config route

セキュリティ アプライアンス上で実行されているルート コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config route** コマンドを使用します。

show running-config [**all**] **route**

構文の説明

デフォルトの動作や値はありません。

デフォルト

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

例

次に、**show running-config route** コマンドの出力例を示します。

```
hostname# show running-config route
route outside 10.30.10.0 255.255.255.0 1
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。

show running-config route-map

ルート マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config route-map** コマンドを使用します。

show running-config route-map [*map_tag*]

構文の説明

map_tag	（任意）ルート マップ タグのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** を追加しました。

使用上のガイドライン

コンフィギュレーション内に定義されたすべてのルート マップを表示するには、**show running-config route-map** コマンドを使用します。名前を指定して個々のルート マップを表示するには、**show running-config route-map** *map_tag* コマンドを使用します。*map_tag* はルート マップの名前です。複数のルート マップで同じマップ タグ名を共有できます。

例

次に、**show running-config route-map** コマンドの出力例を示します。

```
hostname# show running-config route-map
route-map maptag1 permit sequence 10
    set metric 5
    match metric 3
route-map maptag1 permit sequence 12
    set metric 5
    match interface backup
    match metric 3
route-map maptag2 deny sequence 10
    match interface dmz
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。

show running-config router

指定したルーティング プロトコルのグローバル コンフィギュレーション コマンドを表示するには、特権 EXEC モードで **show running-config router** コマンドを使用します。

show running-config [all] **router** [**ospf** [*process_id*] | **rip** | **eigrp** [*as-number*]]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての router コマンドを表示します。
as-number	（任意）指定した EIGRP 自律システム番号のルータ コンフィギュレーション コマンドを表示します。指定されていない場合は、すべての EIGRP ルーティング プロセスのルータ コンフィギュレーション コマンドが表示されます。 セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、オプションの *as-number* 引数を含めても、省略した場合と同じ結果になります。
eigrp	（任意）EIGRP ルータ コンフィギュレーション コマンドを表示します。
ospf	（任意）OSPF ルータ コンフィギュレーション コマンドを表示します。
process_id	（任意）選択した OSPF プロセスに関するコマンドを表示します。
rip	（任意）RIP ルータ コンフィギュレーション コマンドを表示します。

デフォルト

ルーティング プロトコルが指定されていない場合、設定済みのすべてのルーティング プロトコルのルータ コンフィギュレーション コマンドが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show router** コマンドから **show running-config router** コマンドに変更されました。
8.0(2)	このコマンドが、**eigrp** キーワードを含めるように修正されました。

例

次に、**show running-config router ospf** コマンドの出力例を示します。

```
hostname# show running-config router ospf 1

router ospf 1
  log-adj-changes detail
  ignore lsa mospf
  no compatible rfc1583
```

```
  distance ospf external 200
  timers spf 10 20
  timers lsa-group-pacing 60
```

次に、**show running-config router rip** コマンドの出力例を示します。

```
hostname# show running-config router rip

router rip
    network 10.0.0.0
    version 2
    no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての router コマンドをクリアします。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
router ospf	OSPF ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。

show running-config same-security-traffic

セキュリティ レベルが等しいインターフェイス間の通信を表示するには、特権 EXEC モードで **show running-config same-security-traffic** コマンドを使用します。

show running-config same-security-traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show running-config same-security-traffic** コマンドの出力例を示します。

```
hostname# show running-config same-security-traffic
```

関連コマンド

コマンド	説明
same-security-traffic	同じセキュリティ レベルのインターフェイス間の通信を許可します。

show running-config service

システム サービスを表示するには、特権 EXEC モードで **show running-config service** コマンドを使用します。

show running-config service

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** が追加されました。

例

次に、システム サービスを表示するコマンドの例を示します。

```
hostname# show running-config service
service resetoutside
```

関連コマンド

コマンド	説明
service	システム サービスをイネーブルにします。

show running-config service-policy

現在実行されているすべてのサービス ポリシー コンフィギュレーションを表示するには、特権 EXEC モードで **show runnig-config service-policy** コマンドを使用します。

show running-config [all] service-policy

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべてのサービス ポリシー コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config service-policy** コマンドの出力例を示します。

```
hostname# show running-config service-policy
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
service-policy	サービス ポリシーを設定します。
clear service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。

show running-config sla monitor

実行コンフィギュレーションの SLA 動作コマンドを表示するには、特権 EXEC モードで **show running-config sla monitor** コマンドを使用します。

show running-config sla monitor [*sla-id*]

構文の説明

sla_id	表示する **sla monitor** コマンドの SLA ID を指定します。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作の **sla monitor** コマンドが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**sla monitor** コマンド、関連する SLA モニタ コンフィギュレーション モード コマンド、および関連する **sla monitor** スケジュール コマンド（存在する場合）を表示します。コンフィギュレーション内の **track rtr** コマンドは表示しません。

例

次に、**show running-config sla monitor 5** コマンドの出力例を示します。SLA ID が 5 である SLA 動作の SLA モニタ コンフィギュレーションが表示されます。

```
hostname# show running-config sla monitor 5

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
clear configure sla monitor	実行コンフィギュレーションから **sla monitor** コマンドおよび関連コマンドを削除します。
show sla monitor configuration	指定した SLA 動作のコンフィギュレーション値を表示します。

show running-config smtps

smpts の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config smpts** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] smtps

構文の説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config smtps** コマンドの出力例を示します。

```
hostname# show running-config smtps

smtps
server 10.1.1.21
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all smtps

smtps
 port 995
 server 10.1.1.21
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
hostname#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
smtps	SMTPS 電子メール プロキシ コンフィギュレーションを作成または編集します。

show running-config snmp-map

設定されている SNMP マップを表示するには、特権 EXEC モードで **show running-config snmp-map** コマンドを使用します。

show running-config snmp-map *map_name*

構文の説明

map_name	指定した SNMP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config snmp-map コマンドは、設定されている SNMP マップを表示します。

例

次に、**show running-config snmp-map** コマンドの出力例を示します。

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

show running-config snmp-server

現在実行されているすべての SNMP サーバ コンフィギュレーションを表示するには、グローバル コンフィギュレーション モードで **show runnig-config snmp-server** コマンドを使用します。

show running-config [default] snmp-server

構文の説明

default	デフォルトの SNMP サーバ コンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config snmp-server** コマンドの例を示します。

```
hostname# show running-config snmp-server
snmp-server host inside 10.21.104.209 community asa1
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

関連コマンド

コマンド	説明
snmp-server	SNMP サーバを設定します。
clear snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show snmp-server statistics	SNMP サーバ コンフィギュレーションを表示します。

show running-config ssh

現在のコンフィギュレーションの SSH コマンドを表示するには、特権 EXEC モードで **show running-config ssh** コマンドを使用します。

show running-config [**default**] **ssh** [**timeout** | **version**]

show run [**default**] **ssh** [**timeout**]

構文の説明

default	（任意）デフォルトの SSH コンフィギュレーション値および設定されている値を表示します。
timeout	（任意）現在の SSH セッション タイムアウト値を表示します。
version	（任意）現在サポートされている SSH のバージョンを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show ssh** コマンドから **show running-config ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、現在の SSH コンフィギュレーションを表示します。SSH セッションのタイムアウト値だけを表示するには、**timeout** オプションを使用します。アクティブな SSH セッションのリストを表示するには、**show ssh sessions** コマンドを使用します。

例

次に、SSH セッション タイムアウトを表示する例を示します。

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

コマンド	説明
ssh scopy enable	セキュリティ アプライアンスでセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

show running-config ssl

現在の設定済み SSL コマンドのセットを表示するには、特権 EXEC モードで **show running-config ssl** コマンドを使用します。

show running-config ssl

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ssl** コマンドの出力例を示します。

```
hostname# show running-config ssl
ssl server-version  tlsv1
ssl client-version tlsv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作する場合に使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

show running-config static

コンフィギュレーション内のすべての **static** コマンドを表示するには、特権 EXEC モードで **show running-config static** コマンドを使用します。

show running-config static

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** が追加されました。

使用上のガイドライン

このコマンドは、UDP プロトコルの最大接続値を表示します。UDP 最大接続値が「0」の場合、または設定されていない場合、制限は適用されません。

例

次に、コンフィギュレーション内のすべての static コマンドを表示する例を示します。

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```

（注） UDP 接続の制限値は表示されません。

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションからすべての **static** コマンドを削除します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定します。

show running-config sunrpc-server

SunRPC コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config sunrpc-server** コマンドを使用します。

show running-config sunrpc-server *interface_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

構文の説明

interface_name	サーバのインターフェイス。
ip_addr	サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* **-** *port*	SunRPC プロトコルのポート範囲と、2 番めのポート（任意）。
protocol	SunRPC トランスポート プロトコル。
service	サービスを指定します。
service_type	SunRPC サービス プログラム タイプを設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。
TCP	（任意）TCP を指定します。
UDP	（任意）UDP を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

service_type は、**sunrpcinfo** コマンドで指定したものです。

例

次に、**show running-config sunrpc-server** コマンドの出力例を示します。

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから SunRPC サービスをクリアします。
debug sunrpc	SunRPC のデバッグ情報をイネーブルにします。
show conn	SunRPC を含む各種接続タイプの接続状態を表示します。
sunrpc-server	SunRPC サービス テーブルを作成します。
timeout	SunRPC など、さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show running-config sysopt

実行コンフィギュレーションの **sysopt** コマンド コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config sysopt** コマンドを使用します。

show running-config sysopt

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**show sysopt** コマンドから変更されました。

例

次に、**show running-config sysopt** コマンドの出力例を示します。

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

show running-config tcp-map

TCP マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config tcp-map** コマンドを使用します。

show running-config tcp-map [*tcp_map_name*]

構文の説明

tcp_map_name	（任意）TCP マップ名のテキスト。テキストの長さは最大 58 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config tcp-map** コマンドの出力例を示します。

```
hostname# show running-config tcp-map
tcp-map localmap
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。
clear configure tcp-map	TCP マップのコンフィギュレーションをクリアします。

show running-config telnet

セキュリティ アプライアンスへの Telnet 接続の使用を許可されている IP アドレスの現在のリストを表示するには、特権 EXEC モードで **show running-config telnet** コマンドを使用します。また、このコマンドを使用して、Telnet セッションがアイドルになってから、セキュリティ アプライアンスがセッションを閉じるまでの時間（分）を表示することもできます。

show running-config telnet [**timeout**]

構文の説明

timeout	（任意）Telnet セッションがアイドルになってから、セキュリティ アプライアンスがセッションを閉じるまでの時間（分）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **running-config** が追加されました。

例

次に、セキュリティ アプライアンスへの Telnet 接続の使用を許可されている IP アドレスの現在のリストを表示する例を示します。

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

show running-config terminal

現在の端末設定を表示するには、特権 EXEC モードで **show running-config terminal** コマンドを使用します。

show running-config terminal

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ページの長さ設定をクリアする例を示します。

```
hostname# show running-config terminal

Width = 80, no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。

show running-config tftp-server

デフォルト TFTP サーバのアドレスおよびディレクトリを表示するには、グローバル コンフィギュレーション モードで **show running-config tftp-server** コマンドを使用します。

show running-config tftp-server

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**running-config** キーワードが追加されました。

例

次に、デフォルト TFTP サーバの IP/IPv6 アドレスおよびコンフィギュレーション ファイルのディレクトリを表示する例を示します。

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

関連コマンド

コマンド	説明
configure net	指定した TFTP サーバとパスからコンフィギュレーションをロードします。
tftp-server	デフォルト TFTP サーバのアドレスおよびコンフィギュレーション ファイルのディレクトリを設定します。

show running-config threat-detection

脅威の検出のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config threat-detection** コマンドを使用します。

show running-config [**all**] **threat-detection** [**basic-threat** | **rate** | **scanning-threat** | **statistics** [**tcp-intercept**]]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての脅威の検出コマンドを表示します。たとえば、**threat-detection basic-threat** コマンドのデフォルト レート制限を表示できます。
basic-threat	（任意）基本的な脅威に関するコンフィギュレーションを表示します。
rate	（任意）レート コンフィギュレーションを表示します。
scanning-threat	（任意）スキャンによる脅威に関するコンフィギュレーションを表示します。
statistics	（任意）統計情報に関するコンフィギュレーションを表示します。
tcp-intercept	（任意）TCP 代行受信の統計情報に関するコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。

例

次に、**show running-config all threat-detection** コマンドの出力例を示します。この例には、**threat-detection basic-threat** コマンドのデフォルト レート制限が表示されています。

```
hostname# show running-config all threat-detection
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 400 burst-rate 800
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 100 burst-rate 400
```

```
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate scanning-drop rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-drop rate-interval 3600 average-rate 5 burst-rate 10
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 100 burst-rate 200
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 2000 burst-rate 8000
threat-detection scanning-threat shun duration 3600
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show running-config timeout

すべてのプロトコルのタイムアウト値を表示するか、または特定のプロトコルのタイムアウト値だけを表示するには、特権 EXEC モードで **show running-config timeout** コマンドを使用します。

show running-config timeout *protocol*

構文の説明

protocol	（任意）指定したプロトコルのタイムアウト値を表示します。サポートされているプロトコルは、**xlate**、**conn**、**udp**、**icmp**、**rpc**、**h323**、**h225**、**mgcp**、**mgcp-pat**、**sip**、**sip_media**、および **uauth** です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**running-config** および **mgcp-pat** キーワードが追加されました。

例

次に、システムのタイムアウト値を表示する例を示します。

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

関連コマンド

コマンド	説明
clear configure timeout	デフォルトのアイドル時間を復元します。
timeout	アイドル時間の最大継続期間を設定します。

show running-config tls-proxy

現在実行されているすべての TLS プロキシ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config tls-proxy** コマンドを使用します。

show running-config [**all**] **tls-proxy** [*proxy_name*]

構文の説明

all	デフォルトから変更していないコマンドを含め、すべての TLS プロキシ コマンドを表示します。
proxy_name	表示する TLS プロキシの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**show running-config all tls-proxy** コマンドの出力例を示します。

```
hostname# show running-config tls-proxy
tls-proxy proxy
    server trust-point local_ccm
    client ldc issuer ldc_signer
    client ldc key-pair phone_common
    no client cipher-suite
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show tls-proxy	すべての TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

show running-config track

実行コンフィギュレーションの **track rtr** コマンドを表示するには、特権 EXEC モードで **show running-config track** コマンドを使用します。

show running-config track [*track-id*]

構文の説明

track-id	（任意）指定したトラッキング オブジェクト ID を持つ **track rtr** コマンドだけを表示します。

デフォルト

track-id が指定されていない場合、実行コンフィギュレーションのすべての **track rtr** コマンドが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config track** コマンドの出力例を示します。

```
hostname# show running-config track 5

track 5 rtr 124 reachability
```

関連コマンド

コマンド	説明
clear configure track	実行コンフィギュレーションから **track rtr** コマンドを削除します。
show track	追跡対象のオブジェクトに関する情報を表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show running-config tunnel-group

すべてまたは指定したトンネル グループおよびトンネル グループ属性に関するトンネル グループ情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config tunnel-group** コマンドを使用します。

show running-config [**all**] **tunnel-group** [*name* [**general-attributes** | **ipsec-attributes** | **ppp-attributes**]]

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての tunnel-group コマンドを表示します。
general-attributes	一般属性のコンフィギュレーション情報を表示します。
ipsec-attributes	IPSec 属性のコンフィギュレーション情報を表示します。
name	トンネル グループの名前を指定します。
ppp-attributes	PPP 属性のコンフィギュレーション情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•		•		
特権 EXEC	•		•		

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、すべてのトンネル グループの現在のコンフィギュレーションを表示する例を示します。

```
hostname<config># show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname<config>#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ コンフィギュレーションを削除します。
tunnel-group general-attributes	指定したトンネル グループの一般属性を指定するためのサブコンフィギュレーション モードを開始します。

コマンド	説明
tunnel-group ipsec-attributes	指定したトンネル グループの IPSec 属性を指定するためのサブコンフィギュレーション モードを開始します。
tunnel-group	指定されたタイプのトンネル グループ サブコンフィギュレーション モードを開始します。

show running-config url-block

URL フィルタリングで使用するバッファとメモリ割り当てのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-block** コマンドを使用します。

show running-config url-block [**block** | **url-mempool** | **url-size**]

構文の説明

block	バッファされるブロックの最大数に関するコンフィギュレーションを表示します。
url-mempool	URL の最大許容サイズ（KB 単位）に関するコンフィギュレーションを表示します。
url-size	長い URL のバッファに割り当てられるメモリ リソース（KB 単位）に関するコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-block コマンドは、URL フィルタリングで使用するバッファとメモリ割り当てのコンフィギュレーションを表示します。

例

次に、**show running-config url-block** コマンドの出力例を示します。

```
hostname# show running-config url-block
!
url-block block 56
!
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。

コマンド	説明
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config url-cache

URL フィルタリングで使用するキャッシュのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-cache** コマンドを使用します。

show running-config url-cache

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-cache コマンドは、URL フィルタリングで使用するキャッシュのコンフィギュレーションを表示します。

例

次に、**show running-config url-cache** コマンドの出力例を示します。

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config url-server

URL フィルタリング サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-server** コマンドを使用します。

show running-config url-server

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-server コマンドは、URL フィルタリング サーバのコンフィギュレーションを表示します。

例

次に、**show running-config url-server** コマンドの出力例を示します。

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config username

特定のユーザの実行コンフィギュレーションを表示するには、特権 EXEC モードでユーザ名を付加して **show running-config username** コマンドを使用します。すべてのユーザの実行コンフィギュレーションを表示するには、ユーザ名を指定しないでこのコマンドを使用します。

show running-config [**all**] **username** [*name*] [**attributes**]]

構文の説明

attributes	ユーザの特定の AVP を表示します。
all	（任意）デフォルトから変更していないコマンドを含め、すべての username コマンドを表示します。
name	ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、anyuser という名前のユーザに対する show the running-config username コマンドの出力例を示します。

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースをクリアします。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	特定のユーザの属性を設定できます。

show running-config virtual

セキュリティ アプライアンス仮想サーバの IP アドレスを表示するには、特権 EXEC モードで **show running-config virtual** コマンドを使用します。

show running-config [**all**] **virtual**

構文の説明

all	すべての仮想サーバの仮想サーバ IP アドレスを表示します。

デフォルト

all キーワードを省略すると、現在の仮想サーバ（複数可）に明示的に設定されている IP アドレスだけが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

このコマンドを使用するには、特権 EXEC モードを開始しておく必要があります。

例

次に、HTTP 仮想サーバがすでに設定されている場合の **show running-config virtual** コマンドの出力例を示します。

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
virtual	認証仮想サーバのアドレスを表示します。

show running-config vpn load-balancing

現在の VPN ロード バランシングの仮想クラスタ コンフィギュレーションを表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロード バランシング モードで **show running-config vpn-load-balancing** コマンドを使用します。

show running-config [**all**] **vpn load-balancing**

構文の説明

all	デフォルトおよび明示的に設定されている VPN ロード バランシング コンフィギュレーションの両方を表示します。

デフォルト

all キーワードを省略すると、明示的に設定されている VPN ロード バランシング コンフィギュレーションが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—
vpn ロード バランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config vpn load-balancing コマンドは、関連コマンドである **cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、および **priority** に関するコンフィギュレーション情報も表示します。

例

次に、**all** オプションをイネーブルにした **show running-config vpn load-balancing** コマンドとその出力例を示します。

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
 no nat
 priority 9
 interface lbpublic test
 interface lbprivate inside
 no cluster ip address
 no cluster encryption
 cluster port 9023
 no participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド ステートメントを削除します。
show vpn load-balancing	VPN ロード バランシングの実行時統計情報を表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

show running-config webvpn

webvpn の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] webvpn [apcf | auto-signon | cache | proxy-bypass | rewrite | sso-server | url-list]

構文の説明

all	（任意）実行コンフィギュレーションを、デフォルト値を含めて表示します。
apcf	（任意）SSL VPN APCF の実行コンフィギュレーションを表示します。
auto-signon	（任意）SSL VPN 自動サインオンの実行コンフィギュレーションを表示します。
cache	（任意）SSL VPN キャッシングの実行コンフィギュレーションを表示します。
proxy-bypass	（任意）SSL VPN プロキシ バイパスの実行コンフィギュレーションを表示します。
rewrite	（任意）SSL VPN コンテンツ変換の実行コンフィギュレーションを表示します。
sso-server	（任意）シングル サインオンの実行コンフィギュレーションを表示します。
url-list	（任意）URL への SSL VPN アクセスに関する実行コンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが改訂されました。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
WebVPN	•	—	•	—	—

例

次に、**show running-config webvpn** コマンドの出力例を示します。

```
hostname# show running-configuration webvpn
webvpn
 title WebVPN Services for ASA-4
 title-color green
 default-idle-timeout 0
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 authorization-dn-attributes CN
```

次に、**show running-config all webvpn** コマンドの出力例を示します。

```
hostname#(config-webvpn)# show running-config all webvpn

webvpn
 title WebVPN Services for ASA-4
 username-prompt Username
 password-prompt Password
 login-message Please enter your username and password
 logout-message Goodbye
 no logo
 title-color green
 secondary-color #CCCCFF
 text-color white
 secondary-text-color black
 default-idle-timeout 0
 no http-proxy
 no https-proxy
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 no authorization-server-group
 default-group-policy DfltGrpPolicy
 authentication aaa
 no authorization-required
 authorization-dn-attributes CN
hostname#
```

次に、**show running-config webvpn sso-server** コマンドの出力例を示します。

```
hostname#(config-webvpn)# show running-config webvpn sso-server
sso-server
sso-server bxbsvr type siteminder
web-agent-url http://bxb-netegrity.demo.com/vpnauth/
policy-server-secret cisco1234
sso-server policysvr type siteminder
web-agent-url http://webagent1.mysiteminder.com/ciscoauth/
policy-server-secret Cisco1234
max-retry-attempts 4
request-timeout 10
hostname#(config-webvpn)#
```

関連コマンド

コマンド	説明
clear configure webvpn	デフォルト以外のすべての SSL VPN コンフィギュレーション属性を削除します。
debug webvpn	SSL VPN セッションに関するデバッグ情報を表示します。
show webvpn	SSL VPN セッションに関する統計情報を表示します。

show running-config webvpn auto-signon

実行コンフィギュレーションのすべての WebVPN 自動サインオン割り当てを表示するには、グローバル コンフィギュレーション モードで **show running-config webvpn auto-signon** コマンドを使用します。

show running-config webvpn auto-signon

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show running-config webvpn auto-signon** コマンドの出力例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
hostname(config-webvpn)# auto-signon allow uri *.example.com/* auth-type basic
hostname(config-webvpn)# show running-config webvpn auto-signon
auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
auto-signon allow uri *.example.com/* auth-type basic
```

関連コマンド

auto-signon	WebVPN ログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定します。

show running-config zonelabs-integrity

Zone Labs Integrity サーバ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config zonelabs-integrity** コマンドを使用します。

show running-config [**all**] **zonelabs-integrity**

構文の説明

all	（任意）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、すべての Zone Labs Integrity サーバのアドレスおよびアクティブな Zone Labs Integrity サーバに設定されている値を表示します。明示的に設定されている値に加えてデフォルト値も表示するには、**all** パラメータを使用します。

例

次に、**show running-config zonelabs-integrity** コマンドの出力例を示します。

```
hostname# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
hostname#
```

次に、**show running-config all zonelabs-integrity** コマンドの出力例を示します。

```
hostname# show running-config all zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
zonelabs-integrity interface none
zonelabs-integrity fail-open
zonelabs-integrity fail-timeout 10
zonelabs-integrity ssl-client-authentication disable
zonelabs-integrity ssl-certificate-port 80
hostname#
```

関連コマンド

コマンド	説明
clear configure zonelabs-integrity	Zone Labs Integrity サーバのコンフィギュレーションをクリアします。

show running-config vpdn

PPPoE 接続に使用する VPDN コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config vpdn** コマンドを使用します。

show running-config vpdn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、show running-config vpdn コマンドを使用した場合のコマンドの出力例を示します。

```
hostname# show running-config vpdn
vpdn group telecommuters ppp authentication mschap
vpdn username tomm password ********* store-local
```

関連コマンド

コマンド	説明
show running-config vpdn group	VPDN グループの現在のコンフィギュレーションを表示します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

show running-configuration vpn-sessiondb

現在の設定済み vpn-sessiondb コマンドのセットを表示するには、特権 EXEC モードで **show running-configuration vpn-sessiondb** コマンドを使用します。

show running-configuration [all] vpn-sessiondb

構文の説明

all	（任意）デフォルトから変更していないコマンドを含め、すべての **vpn-sessionddb** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

リリース 7.0 以降、このコマンドは VPN セッションの最大数制限のみを表示します（設定されている場合）。

例

次に、**show running-configuration vpn-sessiondb** コマンドの出力例を示します。

```
hostname# show running-configuration vpn-sessiondb
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show running-config wccp

実行コンフィギュレーションの WCCP コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config wccp** コマンドを使用します。

show [**all**] **running-config wccp**

構文の説明

all	1 つまたはすべての WCCP コマンドについて、デフォルトおよび明示的に設定されたコンフィギュレーション情報を表示します。

デフォルト

このコマンドには引数またはキーワードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config wccp** コマンドの出力例を示します。

```
hostname# show running-config wccp
wccp web-cache redirect-list wooster group-list jeeves password whatho
hostname#
```

関連コマンド

コマンド	説明
wccp	WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートを開始します。

CHAPTER 30

show service-policy コマンド～ show xlate コマンド

show service-policy

サービス ポリシー統計情報を表示するには、特権 EXEC モードで **show service-policy** コマンドを使用します。

show service-policy [**global** | **interface** *intf*] [**csc** | **inspect** | **ips** | **police** | **priority** | **shape**]

show service-policy [**global** | **interface** *intf*] [**set connection** [**details**]]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

構文の説明

csc	（任意）**csc** コマンドを含むポリシーだけを出力します。
dest_ip dest_mask	トラフィック フローの宛先 IP アドレスおよびネットマスク。
details	（任意）クライアントごとの接続制限がイネーブルになっている場合は、クライアントごとの接続情報を表示します。
eq *dest_port*	（任意）等号。宛先ポートは、等号に続けて指定するポート番号と一致する必要があります。
eq *src_port*	（任意）等号。送信元ポートは、等号に続けて指定するポート番号と一致する必要があります。
flow *protocol*	（任意）セキュリティ アプライアンスでポリシーの適用対象となるトラフィック フローを指定します。このフローに適用されるポリシーが表示されます。**flow** キーワードに続いて指定する引数とキーワードでは、フローを IP 5 タプル形式で指定します。*protocol* 引数の有効な値については、「使用上のガイドライン」を参照してください。
global	（任意）すべてのインターフェイスに適用されるグローバル ポリシーのみを出力します。
host *dest_host*	トラフィック フローの宛先ホストの IP アドレス。
host *src_host*	トラフィック フローの送信元ホストの IP アドレス。
icmp_control_message	（任意）トラフィック フローの ICMP 制御メッセージを指定します。*icmp_control_message* 引数の有効な値については、「使用上のガイドライン」を参照してください。
icmp_number	（任意）トラフィック フローの ICMP プロトコル番号を指定します。
inspect	（任意）**inspect** コマンドを含むポリシーだけを出力します。
interface *intf*	（任意）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* は **nameif** コマンドで定義したインターフェイス名です。
ips	**ips** コマンドを含むポリシーだけを出力します。
police	**police** コマンドを含むポリシーだけを出力します。
priority	**priority** コマンドを含むポリシーだけを出力します。
set connection	**set connection** コマンドを含むポリシーだけを出力します。
shape	**shape** コマンドを含むポリシーだけを出力します。
src_ip src_mask	トラフィック フローで使用されている送信元 IP アドレスおよびネットマスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**csc** キーワードが追加されました。
7.2(4)/8.0(4)	**shape** キーワードが追加されました。

使用上のガイドライン

flow キーワードを使用すると、記述可能な任意のフローについて、セキュリティ アプライアンスがそのフローに適用するポリシーを特定できます。この情報を利用すると、サービス ポリシー コンフィギュレーションによって、必要なサービスが特定の接続に提供されることを確認できます。**flow** キーワードに続いて指定する引数とキーワードでは、オブジェクト グループ化されていないフローを IP 5 タプル形式で指定します。

IP 5 タプル形式でフローを指定するため、一部の一致基準はサポートされません。次に、フローの検索でサポートされている一致基準のリストを示します。

- **match access-list**
- **match port**
- **match rtp**
- **match default-inspection-traffic**

priority キーワードは、インターフェイスを経由して送信されたパケットの集約カウンタ値を表示するために使用します。

show service-policy コマンドの出力に表示される初期接続の数は、**class-map** コマンドによって定義されたトラフィック マッチングに一致するインターフェイスへの、初期接続の数を示しています。「embryonic-conn-max」フィールドには、Modular Policy Framework を使用するトラフィック クラスに設定された最大初期接続の制限値が表示されます。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続が **class-map** コマンドによって定義されたトラフィック タイプに一致すると、その接続に対して TCP 代行受信が適用されます。

protocol 引数の値

次に、*protocol* 引数の有効な値を示します。

- *number*：プロトコル番号（0 ～ 255）
- **ah**
- **eigrp**
- **esp**
- **gre**
- **icmp**
- **icmp6**

- **igmp**
- **igrp**
- **ip**
- **ipinip**
- **ipsec**
- **nos**
- **ospf**
- **pcp**
- **pim**
- **pptp**
- **snp**
- **tcp**
- **udp**

icmp_control_message 引数の値

次に、*icmp_control_message* 引数の有効な値を示します。

- **alternate-address**
- **conversion-error**
- **echo**
- **echo-reply**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **parameter-problem**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **unreachable**

例

次に、**show service-policy global** コマンドの出力例を示します。

```
hostname# show service-policy global
```

```
Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

次に、**show service-policy priority** コマンドの出力例を示します。

```
hostname# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

次に、**show service-policy flow** コマンドの出力例を示します。

```
hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

次に、**show service-policy inspect http** コマンドの出力例を示します。この例では、match-any クラスマップ内の match コマンドごとに統計情報が表示されます。

```
hostname# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

次に、**show service-policy inspect waas** コマンドの出力例を示します。この例では、waas の統計情報が表示されます。

```
hostname# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
        SYN with WAAS option 4
        SYN-ACK with WAAS option 4
        Confirmed WAAS connections 4
        Invalid ACKs seen on WAAS connections 0
        Data exceeding window size on WAAS connections 0
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	すべてのサービス ポリシー コンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show service-policy inspect ftp

FTP インスペクションの FTP 設定を表示するには、特権 EXEC モードで **show service-policy inspect ftp** コマンドを使用します。

show service-policy [**interface** *int*] **inspect ftp**

構文の説明

interface *int*	（任意）特定のインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

FTP インスペクション中に、セキュリティ アプライアンスが何も通知せずにパケットをドロップする場合があります。セキュリティ アプライアンスの内部でパケットがドロップされているかどうかを確認するには、**show service-policy inspect ftp** コマンドを入力します。

（注） 値が 0 のドロップ カウンタはコマンド出力に表示されません。セキュリティ アプライアンスが何も通知せずにパケットをドロップすることはまれであるため、このコマンドの出力にドロップ カウンタが表示されることはほとんどありません。

表 30-1 に、**show service-policy inspect ftp** コマンドの出力を示します。

表 30-1　FTP ドロップ カウンタの説明

ドロップ カウンタ	カウンタ値の増分条件
Back port is zero drop	APPE、STOR、STOU、LIST、NLIST、RETR の各コマンドを処理するときにポート値が 0 である場合。
Can't allocate back conn drop	別のデータ接続を割り当てようとして失敗した場合。
Can't allocate CP conn drop	セキュリティ アプライアンスが CP 接続のデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないかどうかをチェックしてください。

表 30-1　FTP ドロップ カウンタの説明 （続き）

ドロップ カウンタ	カウンタ値の増分条件
Can't alloc FTP data structure drop	セキュリティ アプライアンスが FTP インスペクションのデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないか確認してください。
Can't allocate TCP proxy drop	セキュリティ アプライアンスが TCP プロキシのデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないか確認してください。
Can't append block drop	FTP パケットのスペース不足により、パケットにデータを追加できない場合。
Can't PAT port drop	セキュリティ アプライアンスがポートに PAT を設定するのに失敗した場合。
Cmd in reply mode drop	REPLY モードでコマンドを受信した場合。
Cmd match failure drop	セキュリティ アプライアンスで regex の照合時に内部エラーが発生した場合。 Cisco TAC にお問い合わせください。
Cmd not a cmd drop	FTP コマンド ストリングに数字などの無効な文字が含まれている場合。
Cmd not port drop	PORT コマンドを受信する予定のセキュリティ アプライアンスで別のコマンドを受信した場合。
Cmd not supported drop	セキュリティ アプライアンスでサポートされていない FTP コマンドを検出した場合。
Cmd not supported in IPv6 drop	IPv6 で FTP コマンドがサポートされていない場合。
Cmd not terminated drop	FTP コマンドが NL または CR で終了した場合。
Cmd retx unexpected drop	再送信されたパケットを予期せずに受信した場合。
Cmd too short drop	FTP コマンドが短すぎる場合。
ERPT too short drop	ERPT コマンドが短すぎる場合。
IDS internal error drop	FTP ID チェック中に内部エラーが発生した場合。 Cisco TAC にお問い合わせください。
Invalid address drop	インスペクション中に無効な IP アドレスが検出された場合。
Invalid EPSV format drop	ESPV コマンドで形式エラーが検出された場合。
Invalid ERPT AF number drop	ERPT コマンドの Address Family（AF; アドレス ファミリ）が無効な場合。
Invalid port drop	インスペクション中に無効なポートが検出された場合。
No back port for data drop	APPE、STOR、STOU、LIST、NLIST、RETR の各コマンドを処理しているときにパケットにポートが含まれていない場合。
PORT command/reply too long drop	PORT コマンドまたはパッシブ応答の長さが 8 を超えた場合。
Reply code invalid drop	応答コードが無効な場合。
Reply length negative drop	応答の長さの値が負である場合。
Reply unexpected drop	セキュリティ アプライアンスで、応答を予期していないときに応答を受信した場合。
Retx cmd in cmd mode drop	CMD モードで再送信されたコマンドを受信した場合。

表 30-1　FTP ドロップ カウンタの説明 （続き）

ドロップ カウンタ	カウンタ値の増分条件
Retx port not old port drop	パケットを再送信したが、パケット内のポートが最初に送信したポートとは異なる場合。
TCP option exceeds limit drop	TCP オプションの長さの値が原因で、オプションの長さが TCP ヘッダーの制限値を超える場合。
TCP option length error drop	TCP オプションの長さの値が正しくない場合。

例

次に、**show service-policy inspect ftp** コマンドの出力例を示します。

```
hostname# show show show service-policy inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ftp, packet 0, drop 0, reset-drop 0
               Can't alloc CP conn drop 1, Can't alloc proxy drop 2
               TCP option exceeds limit drop 3, TCP option length error drop 4
               Can't alloc FTP structure drop 1, Can't append block drop 2
               PORT cmd/reply too long drop 3, ERPT too short drop 4
               Invalid ERPT AF number drop 5, IDS internal error drop 6
               Invalid address drop 7, Invalid port drop 8
               Can't PAT port drop 9, Invalid EPSV format drop 10
               Retx port not old port drop 11, No back port for data drop 12
               Can't alloc back conn drop 13, Back port is zero drop 14
               Cmd too short drop 15, Cmd not terminated drop 16
               Cmd not a cmd drop 17, Cmd match failure drop 18
               Cmd not supported drop 19, Cmd not supported in IPv6 drop 20
               Cmd not port drop 21, Retx cmd in cmd mode drop 22
               Cmd retx unexpected drop 23, Cmd in reply mode drop 24
               Reply length negative drop 25, Reply unexpected drop 26
               Reply code invalid drop 27
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect ftp	FTP トラフィックを検査するアプリケーション インスペクションを設定します。

show service-policy inspect gtp

GTP コンフィギュレーションを表示するには、特権 EXEC モードで **show service-policy inspect gtp** コマンドを使用します。

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **pdpmcb** | **requests** | **statistics** [**gsn** *IP_address*] }

構文の説明

apn	（任意）指定した APN に基づいて、PDP コンテキストの詳細な出力を表示します。
ap_name	統計情報を表示する特定のアクセス ポイント名を指定します。
detail	（任意）PDP コンテキストの詳細な出力を表示します。
imsi	指定した IMSI に基づいて、PDP コンテキストの詳細な出力を表示します。
IMSI_value	統計情報を表示する特定の IMSI を指定するための 16 進数値。
interface	（任意）特定のインターフェイスを指定します。
int	情報を表示するインターフェイスを指定します。
gsn	（任意）GPRS サポート ノードを指定します。このノードは、GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスです。
gtp	（任意）GTP のサービス ポリシーを表示します。
IP_address	統計情報を表示する IP アドレス。
ms-addr	（任意）指定した MS アドレスに基づいて、PDP コンテキストの詳細な出力を表示します。
pdp-context	（任意）パケット データ プロトコル コンテキストを指定します。
pdpmcb	（任意）PDP マスター制御ブロックのステータスを表示します。
requests	（任意）GTP 要求のステータスを表示します。
statistics	（任意）GTP 統計情報を表示します。
tid	（任意）指定した TID に基づいて、PDP コンテキストの詳細な出力を表示します。
tunnel_ID	統計情報を表示する特定のトンネルを指定するための 16 進数値。
version	（任意）GTP バージョンに基づいて、PDP コンテキストの詳細な出力を表示します。
version_num	統計情報を表示する PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

縦棒 | を使用すると、表示内容をフィルタリングできます。表示フィルタリング オプションの詳細については、| を入力してください。

show pdp-context コマンドは、PDP コンテキストに関する情報を表示します。

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、異なる GSN ノードにある 2 個の関連する PDP コンテキストによって定義され、1 つのトンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークとモバイル ステーション ユーザの間でパケットを転送するために必要です。

show gtp requests コマンドは、要求キューに入っている現在の要求を表示します。

例

次に、**show gtp requests** コマンドの出力例を示します。

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦棒 | を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次に、GTP インスペクションの統計情報を表示するコマンドを示します。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次に、PDP コンテキストに関する情報を表示するコマンドを示します。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 30-2 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各列の説明を示します。

表 30-2　PDP コンテキスト

カラムのヘッダー	説明
Version	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr	サービス提供ゲートウェイ サービス ノードを表示します。
Idle	PDP コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。

show service-policy inspect radius-accounting

アプリケーション インスペクションの RADIUS アカウンティング設定を表示するには、特権 EXEC モードで **show service-policy inspect radius-accounting** コマンドを使用します。

show service-policy [**interface** *int*] **inspect radius-accounting**

構文の説明

interface *int*	（任意）特定のインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show show service-policy inspect radius-accounting** コマンドの出力例を示します。

```
hostname# show show service-policy inspect radius-accounting
0 in use, 0 most used, 200 maximum allowed
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect radius-accounting	RADIUS アカウンティング トラフィックを検査するアプリケーション インスペクションを設定します。

show shun

shun 情報を表示するには、特権 EXEC モードで **show shun** コマンドを使用します。

show shun [*src_ip* | *statistics*]

構文の説明

src_ip	（任意）このアドレスに関する情報を表示します。
statistics	（任意）インターフェイスのカウンタだけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show shun** コマンドの出力例を示します。

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。

show sip

SIP セッションを表示するには、特権 EXEC モードで **show sip** コマンドを使用します。

show sip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show sip コマンドは、SIP インスペクション エンジンの問題のトラブルシューティングに役立ちます。説明は、**inspect protocol sip udp 5060** コマンドと一緒にします。**show timeout sip** コマンドは、指示されているプロトコルのタイムアウト値を表示します。

show sip コマンドは、セキュリティ アプライアンスを越えて確立されている SIP セッションの情報を表示します。このコマンドは、**debug sip** および **show local-host** コマンドとともに、SIP インスペクション エンジンの問題のトラブルシューティングに使用されます。

（注）　**pager** コマンドを設定してから **show sip** コマンドを使用することを推奨します。多数の SIP セッション レコードが存在する場合に **pager** コマンドが設定されていないと、**show sip** コマンドが最後まで出力されるまでに時間がかかります。

例

次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 state Active, idle 0:00:06
```

この例では、セキュリティ アプライアンス上の 2 つのアクティブな SIP セッションが表示されています（`Total` フィールドを参照）。各 `call-id` が 1 つのコールを表します。

最初のセッションは call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションがまだコール設定中であることを示しています。コール設定が完了するのは、ACK が確認されてからです。このセッションは、1 秒間アイドル状態でした。

2 番めのセッションは Active 状態です。この状態ではコール設定が完了し、エンドポイントがメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug sip	SIP のデバッグ情報をイネーブルにします。
inspect sip	SIP アプリケーション インスペクションをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show skinny

SCCP（Skinny）インスペクション エンジンの問題をトラブルシューティングするには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）インスペクション エンジンの問題のトラブルシューティングに役立ちます。

例

次の条件での **show skinny** コマンドの出力例を示します。セキュリティ アプライアンスを越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
hostname# show skinny
        LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力から、両方の内部 Cisco IP Phone の間でコールが確立されていることがわかります。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続に関する xlate 情報を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
inspect skinny	SCCP アプリケーション インスペクションをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show sla monitor configuration

デフォルトを含む、SLA 動作のコンフィギュレーション値を表示するには、ユーザ EXEC モードで **show sla monitor configuration** コマンドを使用します。

show sla monitor configuration [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作のコンフィギュレーション値が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションの SLA 動作コマンドを確認するには、**show running config sla monitor** コマンドを使用します。

例

次に、**show sla monitor** コマンドの出力例を示します。SLA 動作 123 のコンフィギュレーション値が表示されます。**show sla monitor** コマンドの出力に続いて、同じ SLA 動作の **show running-config sla monitor** コマンドが出力されます。

```
hostname> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
```

```
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

hostname# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show sla monitor operational-state

SLA 動作の動作状態を表示するには、ユーザ EXEC モードで **show sla monitor operational-state** コマンドを使用します。

show sla monitor operational-state [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作の統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションの SLA 動作コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次に、**show sla monitor operational-state** コマンドの出力例を示します。

```
hostname> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show snmp-server statistics

SNMP サーバ統計情報を表示するには、特権 EXEC モードで **show snmp-server statistics** コマンドを使用します。

show snmp-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

この例は、SNMP サーバ統計情報を表示する方法を示しています。

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
clear configure snmp-server	SNMP サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバ コンフィギュレーションを表示します。

show ssh sessions

セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示するには、特権 EXEC モードで **show ssh sessions** コマンドを使用します。

show ssh sessions [*ip_address*]

構文の説明

ip_address	（任意）指定した IP アドレスのセッション情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

SID は、SSH セッションを識別する一意の番号です。Client IP は、SSH クライアントを実行しているシステムの IP アドレスです。Version は、SSH クライアントがサポートしているプロトコル バージョン番号です。SSH が SSH バージョン 1 だけをサポートしている場合、Version 列には 1.5 が表示されます。SSH クライアントが SSH バージョン 1 と SSH バージョン 2 の両方をサポートしている場合、Version 列には 1.99 が表示されます。SSH クライアントが SSH バージョン 2 だけをサポートしている場合、Version 列には 2.0 が表示されます。Encryption 列には、SSH クライアントが使用している暗号化のタイプが表示されます。State 列には、クライアントとセキュリティ アプライアンスが行っている通信の進行状況が表示されます。[Username] には、このセッションで認証されているログイン ユーザ名が表示されます。Mode 列には、SSH データ ストリームの方向が表示されます。SSH バージョン 2 の場合は、同じ暗号化アルゴリズムを使用することも、異なるアルゴリズムを使用することもできます。Mode フィールドには in および out が表示されます。SSH バージョン 1 の場合は、いずれの方向にも同じ暗号化を使用します。Mode フィールドには該当なしを表す記号（「-」）が表示され、1 つの接続に対して 1 つのエントリのみが表示されます。

例

次に、**show ssh sessions** コマンドの出力例を示します。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

関連コマンド

コマンド	説明
ssh disconnect	アクティブな SSH セッションを切断します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

show startup-config

スタートアップ コンフィギュレーションを表示したり、スタートアップ コンフィギュレーションがロードされたときのエラーを表示したりするには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [errors]

構文の説明

errors	（任意）セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたエラーを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム[1]
特権 EXEC	•	•	•	•	•

1. **errors** キーワードは、シングル モードおよびシステム実行スペースでだけ使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	**errors** キーワードが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドを実行すると、現在の実行スペース（システム コンフィギュレーションまたはセキュリティ コンテキスト）のスタートアップ コンフィギュレーションが表示されます。

スタートアップ エラーをメモリからクリアするには、**clear startup-config errors** コマンドを使用します。

例

次に、**show startup-config** コマンドの出力例を示します。

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
```

```
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

次に、**show startup-config errors** コマンドの出力例を示します。

```
hostname# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "  limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', " nameif inside"
.....
*** Output from config line 37, "  config-url disk:/admin..."
```

関連コマンド

コマンド	説明
clear startup-config errors	スタートアップ エラーをメモリからクリアします。
show running-config	実行コンフィギュレーションを表示します。

show sunrpc-server active

Sun RPC サービス用に開いているピンホールを表示するには、特権 EXEC モードで **show sunrpc-server active** コマンドを使用します。

show sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show sunrpc-server active コマンドは、NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するために使用します。

例

Sun RPC サービスで開かれているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスからの Sun リモート プロセッサ コール サービスをクリアします。
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールをクリアします。
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。

show switch mac-address-table

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルでは、特権 EXEC モードで **show switch mac-address-table** コマンドを使用して、スイッチ MAC アドレス テーブルを表示します。

show switch mac-address-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。スイッチ MAC アドレス テーブルには、スイッチ ハードウェア内の各 VLAN のトラフィックに適用する MAC アドレスとスイッチ ポートのマッピングが保持されます。トランスペアレント ファイアウォール モードでは、**show mac-address-table** コマンドを使用して ASA ソフトウェア内のブリッジ MAC アドレス テーブルを表示します。このブリッジ MAC アドレス テーブルには、VLAN 間を通過するトラフィックに適用する MAC アドレスと VLAN インターフェイスのマッピングが保持されます。

MAC アドレス エントリは 5 分経過するとエージング アウトします。

例

次に、**show switch mac-address-table** コマンドの出力例を示します。

```
hostname# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
-------------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

表 30-3 に、各フィールドの説明を示します。

表 30-3　show switch mac-address-table のフィールド

フィールド	説明
Mac Address	MAC アドレスを表示します。
VLAN	MAC アドレスに関連付けられている VLAN を表示します。
Type	MAC アドレスを、ダイナミックに学習するか、スタティック マルチキャスト アドレスとして学習するか、またはスタティックに学習するかを示します。スタティック エントリは、内部バックプレーン インターフェイスの場合にのみ該当します。
Age	MAC アドレス テーブル内にあるダイナミック エントリの経過時間を表示します。
Port	この MAC アドレスのホストに到達できるスイッチ ポートを表示します。

関連コマンド

コマンド	説明
show mac-address-table	組み込みスイッチのないモデルの MAC アドレス テーブルを表示します。
show switch vlan	VLAN と物理 MAC アドレスの関連付けを表示します。

show switch vlan

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルでは、特権 EXEC モードで **show switch vlan** コマンドを使用して、VLAN および関連付けられているスイッチ ポートを表示します。

show switch vlan

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。他のモデルの場合は、**show vlan** コマンドを使用します。

例

次に、**show switch vlan** コマンドの出力例を示します。

```
hostname# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

表 30-4 に、各フィールドの説明を示します。

表 30-4　show switch vlan のフィールド

フィールド	説明
VLAN	VLAN 番号を表示します。
Name	VLAN インターフェイスの名前を表示します。**nameif** コマンドを使用して名前が設定されていない場合、または **interface vlan** コマンドが実行されていない場合は、ダッシュ（-）が表示されます。
Status	スイッチ内の VLAN とトラフィックを送受信するためのステータス（up または down）を表示します。VLAN がアップ状態になるには、その VLAN で少なくとも 1 つのスイッチ ポートがアップ状態である必要があります。
Ports	各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN にリストされている場合、そのポートはトランク ポートです。上記の出力例で、Ethernet 0/1 は VLAN 100 および VLAN 300 を伝送するトランク ポートです。

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show vlan	組み込みスイッチのないモデルの VLAN を表示します。
switchport mode	スイッチ ポートのモードをアクセス モードまたはトランク モードに設定します。

show tcpstat

セキュリティ アプライアンスの TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを（デバッグのために）表示するには、特権 EXEC モードで **show tcpstat** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show tcpstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを表示できます。表 28 に、表示される TCP 統計情報の説明を示します。

表 30-5　show tcpstat コマンドの TCP 統計情報

統計	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可で使用されます。
tcp_xmt pkts	TCP スタックが送信したパケットの数。
tcp_rcv good pkts	TCP スタックが受信した正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	チェックサムに誤りがあった受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザをハッシュ テーブルに追加しようとしたとき、そのユーザがすでにテーブル内に存在していた回数。
tcp user srch hash hit	検索時にハッシュ テーブル内で TCP ユーザが検出された回数。

表 30-5　show tcpstat コマンドの TCP 統計情報 （続き）

統計	説明
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザが検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたとき、そのユーザがハッシュ テーブル内で検出されなかった回数。
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態（RFC 793 を参照）。表示される値は次のとおりです。 1　CLOSED 2　LISTEN 3　SYN_SENT 4　SYN_RCVD 5　ESTABLISHED 6　FIN_WAIT_1 7　FIN_WAIT_2 8　CLOSE_WAIT 9　CLOSING 10　LAST_ACK 11　TIME_WAIT
rexqlen	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値（ミリ秒）。
to_timer	TCP ユーザの非アクティビティ タイムアウト タイマーの値（ミリ秒）。
cl_timer	TCP ユーザのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザの持続タイマーの値（ミリ秒）。
rt_timer	TCP ユーザの再送信タイマーの値（ミリ秒）。
tries	TCP ユーザの再送信回数。

例

次に、セキュリティ アプライアンスの TCP スタックのステータスを表示する例を示します。

```
hostname# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
```

```
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [**detail** | **file** | **no-config**]

構文の説明

detail	（任意）詳細情報を表示します。
file	（任意）コマンドの出力をファイルに書き込みます。
no-config	（任意）実行コンフィギュレーションの出力を除外します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	**detail** キーワードおよび **file** キーワードが追加されました。
7.2(1)	出力表示が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。テクニカル サポート アナリストは、このコマンドと各種 **show** コマンドの出力を組み合わせてさまざまな情報を入手します。

例

次に、実行コンフィギュレーションの出力を除外して、テクニカル サポートでの分析に使用する情報を表示する例を示します。

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
```

```
0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Apr 17 2005

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------      ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
```

```
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show cpu hogging process ------------------

Process:      fover_parse, NUMHOG: 2, MAXHOG: 280, LASTHOG: 140
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           11a4d5
Traceback:    12135e  121893  121822  a10d8b  9fd061  114de6 113e56f
              777135  7a3858  7a3f59  700b7f  701fbf  14b984

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 XXX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 XXX/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 XXX/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 XXX/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 XXX/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 XXX/intf2
```

```
H*  0011d7f7 0009ff2c 0053e5b0        780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
```

```
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

関連コマンド

コマンド	説明
show clock	Syslog サーバ（PFSS）および Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータスおよびアクティブになっているセキュリティ アプライアンスを表示します。
show memory	物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	セキュリティ アプライアンスのパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	セキュリティ アプライアンス上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにすると、特権 EXEC モードで **show threat-detection rate** コマンドを使用して統計情報を表示できます。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

構文の説明

acl-drop	（任意）アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
bad-packet-drop	（任意）パケット形式に誤りがあって（invalid-ip-header または invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレートを表示します。
conn-limit-drop	（任意）接続制限（システム全体のリソース制限および設定された制限の両方）を超えたためにドロップされたパケットのレートを表示します。
dos-drop	（任意）DoS 攻撃（無効な SPI やステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレートを表示します。
fw-drop	（任意）基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	（任意）疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。
inspect-drop	（任意）アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。
interface-drop	（任意）インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。
scanning-threat	（任意）スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	（任意）TCP SYN 攻撃やデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 10 分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection rate** コマンドの出力例を示します。

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにした場合は、特権 EXEC モードで **show threat-detection scanning-threat** コマンドを使用すると、攻撃者および攻撃対象と分類されたホストが表示されます。

show threat-detection scanning-threat [**attacker** | **target**]

構文の説明

attacker	（任意）攻撃元ホストの IP アドレスを表示します。
target	（任意）攻撃対象ホストの IP アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	見出しテキストに「& Subnet List」を表示するように変更されました。

例

次に、**show threat-detection scanning-threat** コマンドの出力例を示します。

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection shun	現在回避されているホストを表示します。

コマンド	説明
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection shun

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにし、攻撃元ホストを自動的に回避した場合は、特権 EXEC モードで **show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

show threat-detection shun

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドの出力例を示します。

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection statistics host

threat-detection statistics host コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics host** コマンドを使用するとホスト統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定のホストの統計情報を表示します。
mask	（任意）ホスト IP アドレスのサブネット マスクを設定します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:              2938               0       0             10580308
  8-hour Sent byte:               367               0       0             10580308
 24-hour Sent byte:               122               0       0             10580308
  1-hour Sent pkts:                28               0       0               104043
  8-hour Sent pkts:                 3               0       0               104043
 24-hour Sent pkts:                 1               0       0               104043
  20-min Sent drop:                 9               0       1                10851
  1-hour Sent drop:                 3               0       1                10851
  1-hour Recv byte:              2697               0       0              9712670
  8-hour Recv byte:               337               0       0              9712670
 24-hour Recv byte:               112               0       0              9712670
  1-hour Recv pkts:                29               0       0               104846
  8-hour Recv pkts:                 3               0       0               104846
 24-hour Recv pkts:                 1               0       0               104846
  20-min Recv drop:                42               0       3                50567
  1-hour Recv drop:                14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                 0               0       0                  614
  8-hour Sent byte:                 0               0       0                  614
 24-hour Sent byte:                 0               0       0                  614
  1-hour Sent pkts:                 0               0       0                    6
  8-hour Sent pkts:                 0               0       0                    6
 24-hour Sent pkts:                 0               0       0                    6
  20-min Sent drop:                 0               0       0                    4
  1-hour Sent drop:                 0               0       0                    4
  1-hour Recv byte:                 0               0       0                  706
  8-hour Recv byte:                 0               0       0                  706
 24-hour Recv byte:                 0               0       0                  706
  1-hour Recv pkts:                 0               0       0                    7
```

表 30-6 に、各フィールドの説明を示します。

表 30-6　show threat-detection statistics host のフィールド

フィールド	説明
Host	ホストの IP アドレスを表示します。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数を表示します。
act-ses	ホストが現在関係しているアクティブなセッションの合計数を表示します。

表 30-6　show threat-detection statistics host のフィールド （続き）

フィールド	説明
fw-drop	ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、およびデータなし UDP 攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。
null-ses	ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバからデータの送信がなかった UDP セッションです。
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌル セッション状態（上記を参照）であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。

表 30-6　show threat-detection statistics host のフィールド （続き）

フィールド	説明
Total events	各レート間隔におけるイベントの合計数を表示します。現在途中である未完了のバースト間隔は、合計イベント数には含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ホストから正常に送信されたバイト数を表示します。
Sent pkts	ホストから正常に送信されたパケット数を表示します。
Sent drop	ホストから送信されたパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。
Recv byte	ホストが正常に受信したバイト数を表示します。
Recv pkts	ホストが正常に受信したパケット数を表示します。
Recv drop	ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics port

threat-detection statistics port コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics port** コマンドを使用すると、TCP ポートおよび UDP ポートの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]

構文の説明

start_port[**-***end_port*]	（任意）0 ～ 65535 の間の特定のポートまたはポート範囲の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics port** コマンドの出力例を示します。

```
hostname# show threat-detection statistics port

                          Average(eps)     Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939                0       0             10580922
  8-hour Sent byte:                367            22043       0             10580922
 24-hour Sent byte:                122             7347       0             10580922
  1-hour Sent pkts:                 28                0       0               104049
  8-hour Sent pkts:                  3              216       0               104049
 24-hour Sent pkts:                  1               72       0               104049
  20-min Sent drop:                  9                0       2                10855
  1-hour Sent drop:                  3                0       2                10855
  1-hour Recv byte:               2698                0       0              9713376
  8-hour Recv byte:                337            20236       0              9713376
 24-hour Recv byte:                112             6745       0              9713376
  1-hour Recv pkts:                 29                0       0               104853
  8-hour Recv pkts:                  3              218       0               104853
 24-hour Recv pkts:                  1               72       0               104853
  20-min Recv drop:                 24                0       2                29134
  1-hour Recv drop:                  8                0       2                29134
```

表 30-7 に、各フィールドの説明を示します。

表 30-7　show threat-detection statistics port のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。

表 30-7　show threat-detection statistics port のフィールド （続き）

フィールド	説明
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
tot-ses	このポートのセッションの合計数を表示します。
act-ses	ポートが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ポートから正常に送信されたバイト数を表示します。
Sent pkts	ポートから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、ポートから送信されたパケット数を表示します。
Recv byte	ポートが正常に受信したバイト数を表示します。
Recv pkts	ポートが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、ポートが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics protocol

threat-detection statistics protocol コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics protocol** コマンドを使用すると、IP プロトコルの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

構文の説明

protocol_number	（任意）0 ～ 255 の間の特定のプロトコル番号の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
protocol_name	（任意）特定のプロトコル名の統計情報を表示します。 • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン　ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例　次に、**show threat-detection statistics protocol** コマンドの出力例を示します。

```
hostname# show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

表 30-8 に、各フィールドの説明を示します。

表 30-8　show threat-detection statistics protocol のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
protocol_number/ *protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。
tot-ses	このプロトコルのセッションの合計数を表示します。
act-ses	プロトコルが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	プロトコルから正常に送信されたバイト数を表示します。
Sent pkts	プロトコルから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、プロトコルから送信されたパケット数を表示します。
Recv byte	プロトコルが正常に受信したバイト数を表示します。

表 30-8　show threat-detection statistics protocol のフィールド （続き）

フィールド	説明
Recv pkts	プロトコルが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、プロトコルが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics top

threat-detection statistics コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics top** コマンドを使用すると、上位 10 件の統計情報が表示されます。特定のタイプで脅威の検出の統計情報がイネーブルでない場合、このコマンドではそれらの統計情報を表示できません。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**]]

構文の説明

access-list	（任意）許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
all	（任意）TCP 代行受信の場合、追跡されたすべてのサーバの履歴データを表示します。
detail	（任意）TCP 代行受信の場合、サンプリング データの履歴を表示します。
host	（任意）一定期間ごとに上位 10 件のホスト統計情報を表示します。 **（注）** 脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
port-protocol	（任意）TCP/UDP ポート タイプと IP プロトコル タイプを組み合わせた上位 10 件の統計情報を表示します。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
rate-1	（任意）表示されている一定レート間隔のうち、最小のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-1** キーワードを使用すると、1 時間間隔だけがセキュリティ アプライアンスに表示されます。
rate-2	（任意）表示されている一定レート間隔のうち、中間のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-2** キーワードを使用すると、8 時間間隔だけがセキュリティ アプライアンスに表示されます。

rate-3	（任意）表示されている一定レート間隔のうち、最大のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-3** キーワードを使用すると、24 時間間隔だけがセキュリティ アプライアンスに表示されます。
tcp-intercept	TCP 代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバが含まれます。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	**変更内容**
8.0(2)	このコマンドが導入されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics top access-list** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top access-list

                    Top     Average(eps)     Current(eps) Trigger         Total events
```

```
1-hour ACL hits:
            100/3[0]              173              0        0              623488
            200/2[1]               43              0        0              156786
            100/1[2]               43              0        0              156786
8-hour ACL hits:
            100/3[0]               21           1298        0              623488
            200/2[1]                5            326        0              156786
            100/1[2]                5            326        0              156786
```

表 30-9 に、各フィールドの説明を示します。

表 30-9　show threat-detection statistics top access-list のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、時間内の ACE のランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示される ACE が 10 件未満となります。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明の例では、現在のレートは 3:19:30 から 3:20:00 となります。
Trigger	アクセス リスト トラフィックがトリガーするレート制限は設定されていないため、この列は常に 0 です。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
1-hour、8-hour	これらの固定レート間隔における統計情報を表示します。
acl_name/*line_number*	拒否される原因となった ACE のアクセス リスト名および行番号を表示します。

次に、**show threat-detection statistics top access-list rate-1** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top access-list rate-1

                    Top     Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
               100/3[0]              173               0       0               623488
               200/2[1]               43               0       0               156786
               100/1[2]               43               0       0               156786
```

次に、**show threat-detection statistics top port-protocol** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top port-protocol

Top           Name    Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1          gopher    70              71               0       0          32345678
 2   btp-clnt/dhcp    68              68               0       0          27345678
 3          gopher    69              65               0       0          24345678
 4     Protocol-96 * 96              63               0       0          22345678
 5       Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7      Port-8191-65535              55               0       0          12345678
 8            SMTP  366              34               0       0           3345678
 9          IPinIP *  4              30               0       0           2345678
10           EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

表 30-10 に、各フィールドの説明を示します。

表 30-10　show threat-detection statistics top port-protocol のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるポートまたはプロトコルのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるポート / プロトコルが 10 件未満となります。
Name	ポートまたはプロトコル名を表示します。
Id	ポート ID 番号またはプロトコル ID 番号を表示します。アスタリスク（*）は、その ID が IP プロトコル番号であることを意味します。
Average(eps)	表 30-6 の説明を参照してください。
Current(eps)	表 30-6 の説明を参照してください。

表 30-10　show threat-detection statistics top port-protocol のフィールド （続き）

フィールド	説明
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	表 30-6 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたポートおよびプロトコルから正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたポートおよびプロトコルから正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたポートおよびプロトコルから送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたポートおよびプロトコルで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
protocol_number/*protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。

次に、**show threat-detection statistics top host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top host

                  Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
         10.0.0.1[0]             2938                0       0             10580308
  1-hour Sent pkts:
         10.0.0.1[0]               28                0       0               104043
  20-min Sent drop:
         10.0.0.1[0]                9                0       1                10851
  1-hour Recv byte:
         10.0.0.1[0]             2697                0       0              9712670
  1-hour Recv pkts:
         10.0.0.1[0]               29                0       0               104846
  20-min Recv drop:
         10.0.0.1[0]               42                0       3                50567
  8-hour Sent byte:
         10.0.0.1[0]              367                0       0             10580308
  8-hour Sent pkts:
         10.0.0.1[0]                3                0       0               104043
  1-hour Sent drop:
         10.0.0.1[0]                3                0       1                10851
  8-hour Recv byte:
         10.0.0.1[0]              337                0       0              9712670
  8-hour Recv pkts:
         10.0.0.1[0]                3                0       0               104846
  1-hour Recv drop:
         10.0.0.1[0]               14                0       1                50567
```

```
24-hour Sent byte:
         10.0.0.1[0]             122              0       0             10580308
24-hour Sent pkts:
         10.0.0.1[0]               1              0       0               104043
24-hour Recv byte:
         10.0.0.1[0]             112              0       0              9712670
24-hour Recv pkts:
         10.0.0.1[0]               1              0       0               104846
```

表 30-11 に、各フィールドの説明を示します。

表 30-11　show threat-detection statistics top host のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるホストのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるホストが 10 件未満となります。
Average(eps)	表 30-6 の説明を参照してください。
Current(eps)	表 30-6 の説明を参照してください。
Trigger	表 30-6 の説明を参照してください。
Total events	表 30-6 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたホストに正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたホストに正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたホストに送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたホストで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
host_ip_address	パケットまたはバイトが送信、受信、ドロップされたホスト IP アドレスを表示します。

次に、**show threat-detection statistics top tcp-intercept** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2     192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3     192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4     192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5     192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6     192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7     192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8     192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9     192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
```

```
10    192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

表 30-12 に、各フィールドの説明を示します。

表 30-12　show threat-detection statistics top tcp-intercept のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにセキュリティ アプライアンスがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。この間隔の間に、セキュリティ アプライアンスはデータを 60 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常に 60 で割ったレート間隔です。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	サンプリング期間中の平均攻撃レートを 1 秒あたりの攻撃数で表示します。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip	攻撃者の IP アドレスを表示します。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。

次に、**show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (60 Samplings):
              95348      95337      95341      95339      95338      95342
              95337      95348      95342      95338      95339      95340
              95339      95337      95342      95348      95338      95342
              95337      95339      95340      95339      95347      95343
              95337      95338      95342      95338      95337      95342
              95348      95338      95342      95338      95337      95343
              95337      95349      95341      95338      95337      95342
              95338      95339      95338      95350      95339      95570
              96351      96351      96119      95337      95349      95341
              95338      95337      95342      95338      95338      95342
......
```

表 30-13 に、各フィールドの説明を示します。

表 30-13　show threat-detection statistics top tcp-intercept detail のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにセキュリティ アプライアンスがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。この間隔の間に、セキュリティ アプライアンスはデータを 60 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常に 60 で割ったレート間隔です。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	**threat-detection statistics tcp-intercept rate-interval** コマンドで設定されたレート間隔での平均攻撃レートを、1 秒あたりの攻撃数で表示します（デフォルトのレート間隔は 30 分です）。レート間隔中、セキュリティ アプライアンスは 30 秒ごとにデータをサンプリングします。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip or <*various*> Last: *attacker_ip*	攻撃者の IP アドレスを表示します。複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。
sampling data	60 個のサンプリング データ値をすべて表示します。これらの値は、間隔ごとの攻撃数を示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show tls-proxy

TLS プロキシおよびセッション情報を表示するには、グローバル コンフィギュレーション モードで **show tls-proxy** コマンドを使用します。

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**]]

構文の説明

cert-dump	ローカル ダイナミック証明書をダンプします。出力は LDC の 16 進ダンプです。
count	セッション カウンタだけを表示します。
detail	各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。
host *host_addr*	関連付けられたセッションを表示する特定のホストを指定します。
session	アクティブな TLS プロキシ セッションを表示します。
tls_name	表示する TLS プロキシの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**show tls-proxy** コマンドの出力例を示します。

```
hostname# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

次に、**show tls-proxy session** コマンドの出力例を示します。

```
hostname# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

次に、**show tls-proxy session detail** コマンドの出力例を示します。

```
hostname# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show running-config tls-proxy	すべてまたは指定された TLS プロキシの実行コンフィギュレーションを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

show track

トラッキング プロセスが追跡したオブジェクトに関する情報を表示するには、ユーザ EXEC モードで **show track** コマンドを使用します。

show track [*track-id*]

構文の説明

track-id	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

track-id が指定されなかった場合は、すべてのトラッキング オブジェクトに関する情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show track** コマンドの出力例を示します。

```
hostname(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

関連コマンド

コマンド	説明
show running-config track	実行コンフィギュレーションの **track rtr** コマンドを表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show traffic

インターフェイスの送信アクティビティと受信アクティビティを表示するには、特権 EXEC モードで **show traffic** コマンドを使用します。

show traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5550 適応型セキュリティ アプライアンスのための特別な表示が追加されました。

使用上のガイドライン

show traffic コマンドは、show traffic コマンドが最後に入力された時点またはセキュリティ アプライアンスがオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、セキュリティ アプライアンスが直前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

ASA 5550 適応型セキュリティ アプライアンスの場合、**show traffic** コマンドを実行するとスロットごとの集約スループットも表示されます。ASA 5550 適応型セキュリティ アプライアンスのスループットを最大にするには、トラフィックをスロットに均一に分散する必要があります。この表示は、トラフィックが均一に分散しているかどうかを確認するのに役立ちます。

例

次に、**show traffic** コマンドの出力例を示します。

```
hostname# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
```

```
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

ASA 5550 適応型セキュリティ アプライアンスの場合、次のテキストが最後に表示されます。

```
---------------------------------------
        Per Slot Throughput Profile
---------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|***************
    Slot 1:       3149  50%|***************

  Bytes-per-second profile:
    Slot 0:     427044  50%|***************
    Slot 1:     427094  50%|***************
```

関連コマンド

コマンド	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。

show uauth

現在認証済みの 1 名またはすべてのユーザ、ユーザがバインドされているホスト IP、およびキャッシュされた IP とポートの認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

show uauth [*username*]

構文の説明

username	（任意）表示するユーザ認証情報とユーザ認可情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認可情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show uauth コマンドは、1 名またはすべてのユーザの AAA 認可キャッシュおよび認証キャッシュを表示します。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、セキュリティ アプライアンスではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

show uauth コマンドの出力には、認証と認可のために認可サーバに渡されたユーザ名、そのユーザ名がバインドされている IP アドレス、およびこのユーザが認証されたのみであるか、または、キャッシュされたサービスがあるかが表示されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成できません。AAA 認可またはアカウンティ

ング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、いずれのユーザも認証されておらず、かつ、1 つのユーザ認証が進行している場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

次に、3 人のユーザが認証されており、かつ、セキュリティ アプライアンスを介してサービスを使用することが認可されている場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

関連コマンド

コマンド	説明
clear uauth	現在のユーザの認証情報と認可情報を削除します。
timeout	アイドル時間の最大継続期間を設定します。

show url-block

url-block バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

show url-block [**block statistics**]

構文の説明

block statistics	（任意）ブロック バッファの使用状況に関する統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show url-block block statistics コマンドは、URL ブロック バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示します。

例

次に、**show url-block** コマンドの出力例を示します。

```
hostname# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

URL ブロック バッファのコンフィギュレーションが表示されています。

次に、**show url-block block statistics** コマンドの出力例を示します。

```
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-cache statistics

N2H2 または Websense のフィルタリング サーバから受信した URL 応答に使用される URL キャッシュの情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

show url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show url-cache statistics コマンドには、次のエントリが表示されます。

- Size：キャッシュ サイズ（KB 単位）。**url-cache** *size* オプションを使用して設定します。
- Entries：キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use：キャッシュに含まれる現在のエントリ数。
- Lookups：セキュリティ アプライアンスがキャッシュ エントリを検索した回数。
- Hits：セキュリティ アプライアンスがキャッシュ内でエントリを検出した回数。

show perfmon コマンドを使用すると、N2H2 Sentian または Websense のフィルタリング アクティビティに関する追加情報を表示できます。

例

次に、**show url-cache statistics** コマンドの出力例を示します。

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 Hits :     290
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバから受信した応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-server

URL フィルタリング サーバに関する情報を表示するには、特権 EXEC モードで **show url-server** コマンドを使用します。

show url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバのベンダーおよびステータスを表示します。また、URL、HTTPS 接続、および TCP 接続について、合計数、許可された数、拒否された数を表示します。

show url-server コマンドには、次の情報が表示されます。

- N2H2 の場合：**url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- Websense の場合：**url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

例

次に、**show url-server statistics** コマンドの出力例を示します。

```
hostname## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
```

```
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                         UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                         DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          411     0
LOOKUP_REQUEST          366519  365952
LOG_REQUEST             0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis.  The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。

url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show version

ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連する動作期間データを表示するには、ユーザ EXEC モードで **show version** コマンドを使用します。

show version

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	ステートフル フェールオーバー モードでは、クラスタの動作期間を示す追加の行が表示されます。

使用上のガイドライン

show version コマンドを使用すると、ソフトウェア バージョン、最後にリブートされてからの動作時間、プロセッサ タイプ、フラッシュ パーティション タイプ、インターフェイス ボード、シリアル番号（BIOS ID）、アクティベーション キー値、ライセンス タイプ（R または UR）、およびコンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

show version コマンドで表示されるシリアル番号は、フラッシュ パーティション BIOS の番号です。この番号は、シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを入手する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

- 以前のリリースにダウングレードした場合、現在のリリースのキーでは、以前のリリースでサポートされている数よりも多くのセキュリティ コンテキストが使用できる場合があります。キーのセキュリティ コンテキストの値がプラットフォームの制限を超えると、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: 50 security contexts exceeds the limit in the
  platform, reduce to 20 security contexts.
  ```

- 以前のリリースにダウングレードした場合、現在のリリースのキーでは GTP/GPRS がイネーブルであるにもかかわらず、以前のリリースでは GTP/GPRS が許可されていないことがあります。キーを使用して GTP/GPRS をイネーブルにしても、GTP/GPRS がソフトウェアのバージョンによって許可されない場合は、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
  GTP/GPRS.
  ```

フェールオーバー クラスタの動作期間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台のユニットが動作を停止しても、アクティブなユニットが動作を継続する限り、動作期間の値は増加し続けます。このため、フェールオーバー クラスタの動作期間を個別のユニットの動作期間よりも長くすることができます。フェールオーバーを一時的にディセーブルにしてから再びイネーブルにすると、フェールオーバーがディセーブルになる前のユニットの稼働時間と、フェールオーバーがディセーブルである間のユニットの稼働時間が加算されて、フェールオーバー クラスタの動作期間がレポートされます。

例

次に、ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連する動作期間の情報を表示する例を示します。ステートフル フェールオーバーが設定されている環境では、フェールオーバー クラスタの動作期間を示す追加の行が表示されます。フェールオーバーが設定されていない場合、この行は表示されません。

```
hostname# show version

Cisco Adaptive Security Appliance Software Version 8.0(0)
Device Manager Version 6.0(0)

Compiled on Mon 16-April-07 03:29 by root
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/main_backup.cfg"

hostname up 2 days 10 hours
failover cluster up 2 days 11 hours

Hardware:   ASA5520, 1024 MB RAM, CPU Pentium 4 Celeron 2000 MHz
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.01
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.04
 0: Ext: GigabitEthernet0/0  : address is 000b.fcf8.c44e, irq 9
 1: Ext: GigabitEthernet0/1  : address is 000b.fcf8.c44f, irq 9
 2: Ext: GigabitEthernet0/2  : address is 000b.fcf8.c450, irq 9
 3: Ext: GigabitEthernet0/3  : address is 000b.fcf8.c451, irq 9
 4: Ext: Management0/0       : address is 000b.fcf8.c44d, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 150
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 10
GTP/GPRS                     : Enabled
VPN Peers                    : 750
WebVPN Peers                 : 500
Advanced Endpoint Assessment : Disabled

This platform has an ASA 5520 VPN Plus license.

Serial Number: P3000000098
Running Activation Key: 0x7c2e394b 0x0c842e53 0x98f3edf0 0x8c1888b0 0x0336f1ac
Configuration register is 0x1
```

```
Configuration last modified by enable_15 at 14:17:59.410 EST Wed April 16 2007
hostname#
```

eject コマンドを実行した後、デバイスが物理的に取り外されていない状態で **show version** コマンドを入力すると、次のメッセージが表示されます。

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

関連コマンド

コマンド	説明
eject	外部コンパクト フラッシュ デバイスを、セキュリティ アプライアンスから物理的に取り外す前にシャットダウンできるようにします。
show hardware	ハードウェアの詳細情報を表示します。
show serial	ハードウェアのシリアル情報を表示します。
show uptime	セキュリティ アプライアンスの稼働時間を表示します。

show vlan

セキュリティ アプライアンスに設定されているすべての VLAN を表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、設定されている VLAN を表示する例を示します。

```
hostname# show vlan
10-11, 30, 40, 300
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show vpn load-balancing

VPN ロード バランシングの仮想クラスタ コンフィギュレーションに関する実行時統計情報を表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロード バランシング モードで **show vpn-load-balancing** コマンドを使用します。

show vpn load-balancing

構文の説明

このコマンドには、変数も引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—
vpn ロード バランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	出力例の Load (%) 表示および Session 表示に、個別の IPSec 列および SSL 列が追加されました。

使用上のガイドライン

show vpn load-balancing コマンドは、仮想 VPN ロード バランシング クラスタに関する統計情報を表示します。ローカル デバイスが VPN ロード バランシング クラスタに参加していない場合、このコマンドはデバイスに VPN ロード バランシングが設定されていないことを通知します。

ロードバランシング クラスタのマスターは、アクティブな AnyConnect セッション、クライアントレス セッション、そして設定された制限またはライセンス数制限に基づく最大許可セッションがあるクラスタ内の各 ASA からメッセージを定期的に受信します。クラスタ内のある ASA の容量が 100% いっぱいであると示される場合、クラスタ マスターはこれに対してさらに接続をリダイレクトすることはできません。ASA がいっぱいであると示されても、ユーザによっては非アクティブまたは再開待ち状態となり、ライセンスを消費する可能性があります。回避策として、セッション合計数ではなく、セッション合計数から非アクティブ状態のセッション数を引いた数が各 ASA によって提供されます つまり、非アクティブなセッションはクラスタ マスターに報告されません。ASA が（非アクティブなセッションによって）いっぱいになっている場合でも、クラスタ マスターは必要に応じて接続を ASA に引き続きリダイレクトします。ASA が新しい接続を受信すると、最も長く非アクティブになっていたセッションがログオフされ、新しい接続がそのライセンスを引き継ぎます。

出力にあるアスタリスク（*）は、接続先のセキュリティ アプライアンスの IP アドレスを示します。

例

次に、ローカル デバイスが VPN ロード バランシング クラスタに参加してい場合の **show vpn load-balancing** コマンドの出力例を示します。

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
                                          Load (%)           Sessions
Public IP       Role   Pri     Model          IPSec  SSL        IPSec   SSL
-------------------------------------------------------------------------------
* 192.168.1.40  Master 10     PIX-515         0       0          0       0
  192.168.1.110  Backup   5 PIX-515          0       0          0       0
hostname(config-load-balancing)#
```

（注） 非アクティブなセッションは最長時間から最短時間の順にソートされます。非アクティブな SSL セッションはカウントされないため、セッションとロードの合計には表示されません。

ローカル デバイスが VPN ロード バランシング クラスタに参加していない場合、**show vpn load-balancing** コマンドには次のような異なる結果が表示されます。

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド ステートメントを削除します。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

show vpn-sessiondb

VPN セッションに関する情報を表示するには、特権 EXEC モードで **vpn-sessiondb** コマンドを使用します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できる他、情報をフィルタリングおよびソートするためのオプションが用意されています。使用可能なオプションについては、「構文の説明」および「使用上のガイドライン」を参照してください。

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* **| webvpn | email-proxy | svc} [filter {name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo* **| inactive}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption | inactivity}]**

構文の説明

表示の詳細度	説明
detail	セッションに関する詳細な情報を表示します。たとえば、IPSec セッションに対して **detail** オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの詳細情報が表示されます。 **detail** および **full** オプションを指定すると、セキュリティ アプライアンスではマシンで読み取り可能な形式で詳細な出力を表示します。
filter *filter_criteria*	（任意）1 つまたは複数のフィルタ オプションを使用して、指定する情報だけを表示するように出力をフィルタリングします。詳細については、「使用上のガイドライン」を参照してください。
full	連続した、短縮されていない出力を表示します。出力のレコード間には | 文字と || ストリングが表示されます。
sort	指定するソート オプションに従って出力をソートします。詳細については、「使用上のガイドライン」を参照してください。
表示するセッション タイプ	**説明**
email-proxy	電子メールプロキシ セッションを表示します。電子メールプロキシ セッションに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**（接続名）、**ipaddress**（クライアント）、**encryption** を使用して情報をフィルタリングすることもできます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号（1 ～ 750）を指定します。フィルタ オプションとソート オプションは適用されません。
l2l	VPN の LAN-to-LAN セッション情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
remote	リモートアクセス セッションを表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションである **name**、**a-ipaddress**、**p-ipaddress**、**tunnel-group**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
webvpn	WebVPN セッションに関する情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**encryption** を使用して情報をフィルタリングすることもできます。
svc	SSL VPN クライアント属性を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.3(0)	VLAN フィールドの説明が追加されました。
7.2(1)	このコマンドが導入されました。
8.0(5)	**filter** オプションとして **inactive** および **sort** オプションとして **inactivity** が追加されました。

使用上のガイドライン

次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ / ソート オプション	説明
filter a-ipaddress *IPaddr*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）に関する情報だけを表示します。
sort a-ipaddress	割り当て済み IP アドレスで表示内容をソートします。
filter encryption *encryption-algo*	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションに関する情報だけを表示します。
sort encryption	暗号化アルゴリズムで表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
filter inactive	接続が切断された非アクティブなセッションをフィルタリングします。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションがアクティブな場合、00:00m:00s が表示されます。
sort inactivity	非アクティブなセッションをソートします。
filter ipaddress *IPaddr*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）に関する情報だけを表示します。
sort ipaddress	内部 IP アドレスで表示内容をソートします。
filter name *username*	出力をフィルタリングして、指定したユーザ名（複数可）のセッションを表示します。
sort name	ユーザ名のアルファベット順に表示内容をソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスに関する情報だけを表示します。
sort p-address	指定した外部 IP アドレス（複数可）で表示内容をソートします。
filter protocol *protocol-name*	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションに関する情報だけを表示します。

フィルタ / ソート オプション	説明
sort protocol	プロトコルで表示内容をソートします。プロトコルには、IKE、IMAP4S、IPSec、IPSecLAN2LAN、IPSecLAN2LANOverNatT、IPSecOverNatT、IPSecoverTCP、IPSecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN が含まれます。
filter tunnel-group *groupname*	出力をフィルタリングして、指定したトンネル グループ（複数可）に関する情報だけを表示します。
sort tunnel-group	トンネル グループで表示内容をソートします。
| 記号	引数 {begin | include | exclude | grep | [-v]} {reg_exp} を使用して、出力を修正します。
<cr>	出力をコンソールに送信します。

特権 EXEC モードで入力した次の例では、LAN-to-LAN セッションに関する詳細な情報を表示しています。

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.1
Index        : 1                    IP Addr      : 172.16.0.1
Protocol     : IPSecLAN2LAN         Encryption   : AES256
Bytes Tx     : 48484156             Bytes Rx     : 875049248
Login Time   : 09:32:03 est Mon Aug 2 2004
Duration     : 6:16:26
Filter Name  :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID   : 1
  UDP Src Port : 500                  UDP Dst Port : 500
  IKE Neg Mode : Main                 Auth Mode    : preSharedKeys
  Encryption   : AES256               Hashing      : SHA1
  Rekey Int (T): 86400 Seconds        Rekey Left(T): 63814 Seconds
  D/H Group    : 5

IPSec:
  Session ID   : 2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256               Hashing      : SHA1
  Encapsulation: Tunnel               PFS Group    : 5
  Rekey Int (T): 28800 Seconds        Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224             Bytes Rx     : 2639672
  Pkts Tx      : 1635314              Pkts Rx      : 37526


IPSec:
  Session ID   : 3
  Local Addr   : 10.0.0.1/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256               Hashing      : SHA1
  Encapsulation: Tunnel               PFS Group    : 5
  Rekey Int (T): 28800 Seconds        Rekey Left(T): 6282 Seconds
  Bytes Tx     : 1619268              Bytes Rx     : 872409912
  Pkts Tx      : 19277                Pkts Rx      : 1596809

hostname#
```

次の例は単一セッションの詳細を示します。

```
AsaNacDev# show vpn-sessiondb detail full index 4
Session Type: Remote Detailed |

Index: 2 | EasyVPN: 0 | Username: uuuu | Group: DfltGrpPolicy | Tunnel Group:
regr3000multigroup | IP Addr: 192.168.2.80 | Public IP: 161.44.173.216 | Protocol:
IPSecOverUDP | Encryption: 3DES | Login Time: 12:51:54 EDT Wed Jun 21 2006 |Duration:
0h:02m:44s | Bytes Tx: 2134 | Bytes Rx: 8535 | Client Type: WinNT | Client Ver: 4.0.5
(Rel) | Filter Name:  | NAC Result: N/A | Posture Token: : | VM Result: Static | VLAN: 10
||

IKE Sessions: 1
 | IPSecOverUDP Sessions: 1
 |

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeys | UDP Source Port: 500 |
UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES | Hashing:
SHA1 | Diffie-Hellman Group: 2 | Rekey Time Interval: 40000 Seconds| Rekey Left(T): 39836
Seconds ||

Type: IPSecOverUDP | Session ID: 2 | Local IP Addr: 0.0.0.0/0.0.0.0/0/0 | Remote IP Addr:
192.168.2.80/255.255.255.255/0/0 | Encryption: 3DES | Hashing: SHA1 | Encapsulation:
Tunnel | UDP Destination Port: 10000 | Rekey Time Interval: 28800 Seconds | Rekey Left(T):
28636 Seconds | Idle Time Out: 30 Minutes | Idle TO Left: 30 Minutes | Bytes Tx: 2134 |
Bytes Rx: 8535 | Packets Tx: 15 | Packets Rx: 2134 | ||

VLAN Mapping: VLAN: 10 |

AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : dbrownhi
Index        : 1
Assigned IP  : 192.168.2.70          Public IP    : 10.86.5.114
Protocol     : IPSec                 Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                     Bytes Rx     : 604533
Client Type  : WinNT                 Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPSec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
```

```
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds           Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                       Bytes Rx     : 604533
  Pkts Tx      : 0                       Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds            Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds             EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds               Posture Token: Healthy
  Redirect URL : www.cisco.com
```

例に示すとおり、**show vpn-sessiondb** コマンドの応答に表示されるフィールドは、入力するキーワードによって異なります。表 30-14 に、これらのフィールドの説明を示します。

表 30-14　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Auth Mode	このセッションを認証するためのプロトコルまたはモード。
Bytes Rx	セキュリティ アプライアンスがリモートのピアまたはクライアントから受信した合計バイト数。
Bytes Tx	セキュリティ アプライアンスがリモートのピアまたはクライアントに送信した合計バイト数。
Client Type	リモート ピア上で実行されるクライアント ソフトウェア（利用できる場合）。
Client Ver	リモート ピア上で実行されるクライアント ソフトウェアのバージョン。
Connection	接続名またはプライベート IP アドレス。
D/H Group	Diffie-Hellman グループ。IPSec SA 暗号キーを生成するためのアルゴリズムおよびキー サイズ。
Duration	セッションのログイン時刻から直前の画面リフレッシュまでの経過時間（HH:MM:SS）。
EAPoUDP Session Age	正常に完了した直前のポスチャ確認からの経過秒数。
Encapsulation	IPSec Encapsulation Security Payload（ESP; 暗号ペイロード）プロトコルの暗号化と認証（つまり、ESP を適用した元の IP パケットの一部）を適用するためのモード。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム（ある場合）。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム。
EoU Age (T)	EAPoUDP セッションの経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
Filter Name	セッション情報の表示を制限するよう指定されたユーザ名。
Hashing	パケットのハッシュを生成するためのアルゴリズム。IPSec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
Hold-Off Time Remaining	直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
IKE Neg Mode	キー情報を交換し、SA を設定するための IKE（IPSec フェーズ 1）モード（アグレッシブまたはメイン）。

表 30-14　show vpn-sessiondb コマンドのフィールド （続き）

フィールド	説明
IKE Sessions	IKE（IPSec フェーズ 1）セッションの数で、通常は 1。これらのセッションにより、IPSec トラフィックのトンネルが確立されます。
Index	このレコードの固有識別情報。
IP Addr	このセッションのリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。
IPSec Sessions	IPSec（フェーズ 2）セッション（トンネル経由のデータ トラフィック セッション）の数。各 IPSec リモート アクセス セッションには、2 つの IPSec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
Local IP Addr	トンネルのローカル エンドポイント（セキュリティ アプライアンス上のインターフェイス）に割り当てられた IP アドレス。
Login Time	セッションがログインした日付と時刻（MMM DD HH:MM:SS）。時刻の表示は 24 時間表示です。
NAC Result	ネットワーク アドミッション コントロール ポスチャ検証の状態。次のいずれかを指定できます。 • [Accepted] : ACS は正常にリモート ホストのポスチャを検証しました。 • [Rejected] : ACS はリモート ホストのポスチャの検証に失敗しました。 • [Exempted] : セキュリティ アプライアンスに設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。 • [Non-Responsive] : リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。 • [Hold-off] : ポスチャ検証に成功した後、セキュリティ アプライアンスとリモート ホストの EAPoUDP 通信が途絶えました。 • [N/A] : VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。 • [Unknown] : ポスチャ検証が進行中です。
NAC Sessions	ネットワーク アドミッション コントロール（EAPoUDP）セッションの数。
Packets Rx	セキュリティ アプライアンスがリモート ピアから受信したパケット数。
Packets Tx	セキュリティ アプライアンスがリモート ピアに送信したパケット数。
PFS Group	完全転送秘密グループ番号。
Posture Token	Access Control Server 上で設定可能な情報テキスト ストリング。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。

表 30-14　show vpn-sessiondb コマンドのフィールド （続き）

フィールド	説明
Redirect URL	ポスチャ検証またはクライアントレス認証に続いて、ACS はセッションのアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。セキュリティ アプライアンスは、リモート ホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、セキュリティ アプライアンスはリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。 Redirect URL は、IPSec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。
Rekey Int (T)	IPSec（IKE）SA 暗号キーの有効期限。
Rekey Left (T)	IPSec（IKE）SA 暗号キーの残りのライフタイム。
Rekey Time Interval	IPSec（IKE）SA 暗号キーの有効期限。
Remote IP Addr	トンネルのリモート エンドポイント（リモート ピア上のインターフェイス）に割り当てられた IP アドレス。
Reval Int (T)	Revalidation Time Interval。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Reval Left (T)	Time Until Next Revalidation。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Session ID	セッション コンポーネント（サブセッション）の ID。各 SA には独自の ID があります。
Session Type	セッションのタイプ（LAN-to-LAN または Remote）。
SQ Int (T)	Status Query Time Interval。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Tunnel Group	属性値を求めるために、このトンネルが参照するトンネル グループの名前。
UDP Dst Port または UDP Destination Port	リモート ピアが使用する UDP のポート番号。

表 30-14　show vpn-sessiondb コマンドのフィールド （続き）

フィールド	説明
UDP Src Port または UDP Source Port	セキュリティ アプライアンスが使用する UDP のポート番号。
Username	セッションを確立したユーザのログイン名。
VLAN	このセッションに割り当てられた出力 VLAN インターフェイス。セキュリティ アプライアンスは、すべてのトラフィックをこの VLAN に転送します。次のいずれかの要素で値を指定します。 • グループ ポリシー • 継承されたグループ ポリシー

関連コマンド

コマンド	説明
show running-configuration vpn-sessiondb	VPN セッション データベースの実行コンフィギュレーションを表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。
show vpn-sessiondb summary	すべての VPN セッションの要約を表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

構文の説明

encryption	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化に関して指定します。暗号化アルゴリズムには次の種類があります。 aes128　des aes192　3des aes256　rc4
filter *groupname*	出力をフィルタリングして、指定するトンネル グループについてのみセッションの比率を表示します。
protocol	表示するプロトコルを指定します。プロトコルには次の種類があります。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、引数として **encryption** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio enc
```

```
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

次に、引数として **protocol** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPSec                    1              20%
IPSecLAN2LAN             0               0%
IPSecLAN2LANOverNatT     0               0%
IPSecOverNatT            0               0%
IPSecOverTCP             1 20%
IPSecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPSec            0               0%
L2TPOverIPSecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show vpn-sessiondb summary

IPSec、Cisco AnyConnect、および NAC の各セッションの数を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

show vpn-sessiondb summary

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.3(0)	VLAN マッピング セッション テーブルが追加されました。
7.2(1)	このコマンドが導入されました。
8.0(5)	アクティブ、累積、ピーク同時、および非アクティブのセッションに関する出力が新たに追加されました。

例

次に、アクティブなデバイス上での **show vpn-sessiondb summary** コマンドの出力例を示します。

（注） スタンバイ状態のデバイスでは、アクティブなセッションと非アクティブなセッションが区別されません。

```
hostname# show vpn-sessiondb summary

Active Session Summary
Sessions:
                  Active :Cumulative :Peak Concurrent :Inactive :
  SSL VPN   :          0 :         1 :               1 :
    Clientless only    0 :         0 :               0 :         0
    With client        6 :         6 :               1 :         4
Totals                 0 :        10

License Information:
    Shared VPN License Information:
        SSL VPN                     : 12000
            Allocated to this device  :    0
            Allocated to network      :    0
            Device limit              : 750

IPsec   :   750     Configured :750    Active : 0     Load : 0%
SSL VPN :   750     Configured :750    Active : 0     Load : 0%
                        Active : Cumulative : Peak Concurrent
```

```
SSL VPN         :           6 :         1 :             1
Totals          :           0 :        10 :

Active NAC Sessions:
  Accepted                : 0
  Rejected                : 0
  Exempted                : 0
  Non-responsive          : 0
Hold-off                : 0
  N/A                     : 0

Active VLAN Mapping Sessions:
  Static                  : 0
  Auth                    : 0
  Access                  : 0
  Guest                   : 0
  Quarantine              : 0
  N/A                     : 0

F1-asa1#
```

セッションとは、特定のピアとの間で確立された VPN トンネルです。IPSec LAN-to-LAN トンネルは 1 セッションとしてカウントされ、このトンネル経由で複数のホスト間接続が可能になります。IPSec リモート アクセス セッションは、1 つのユーザ接続をサポートする 1 リモート アクセス トンネルです。

Active SSL VPN With Client カラムには、データを渡すことのできるアクティブな SSL トンネル セッションの数が表示されます。非アクティブ カラムには SSL トンネル セッションを失っているため、データを渡すことができないセッションが表示されます。非アクティブなセッションは後の時点で接続を再開する場合があります。ロード バランシングのため、非アクティブなセッションはマスターへの負荷として報告されません。たとえば、1 つのクラスタ メンバーに合計 10 件のセッションがあり、うち 6 つがアクティブ、4 つが非アクティブの場合、マスターに報告される負荷は 6 セッションです。

Total SSL VPN カラムには、アクティブなセッションと非アクティブなセッションの両方が表示されます。

（注） アクティブなセッションも非アクティブなセッションも、これまでと同様にライセンスを必要とします。デバイスの既存のセッションは、状態に関係なくライセンスを必要とします。

SSL VPN With Client の Cumulative 列には、確立されているアクティブなセッションの数が表示されます。SSL VPN With Client の Peak Concurrent 列には、データを送信中で、同時にアクティブなセッションのピーク数が表示されます。

表 30-15 に、Active Sessions テーブルと Session Information テーブルにあるフィールドの説明を示します。

表 30-15　show vpn-sessiondb summary コマンド：Active Sessions および Session Information のフィールド

フィールド	説明
Concurrent Limit	このセキュリティ アプライアンス上で許可された、同時にアクティブなセッションの最大数。
Cumulative Sessions	セキュリティ アプライアンスが最後に起動またはリセットされたとき以降のすべてのタイプのセッション数。
LAN-to-LAN	現在アクティブな IPSec LAN-to-LAN セッションの数。

表 30-15　show vpn-sessiondb summary コマンド：Active Sessions および Session Information のフィールド（続き）

フィールド	説明
Peak Concurrent	セキュリティ アプライアンスが最後に起動またはリセットされたとき以降に同時にアクティブであった、すべてのタイプのセッションの最大数。
Percent Session Load	使用中の vpn セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。利用可能なセッションの最大数は、次のいずれかの値です。 • ライセンスのある IPSec セッションおよび SSL VPN セッションの最大数 • 次のコマンドを使用して設定されたセッションの最大数 – **vpn-sessiondb max-session-limit** – **vpn-sessiondb max-webvpn-session-limit**
Remote Access	現在アクティブな PPTP、L2TP、IPSec リモート アクセス ユーザ、L2TP over IPSec、および IPSec through NAT の各セッションの数。
Total Active Sessions	現在アクティブなすべてのタイプのセッションの数。

Active NAC Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative NAC Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 30-16 に、Active NAC Sessions テーブルおよび Total Cumulative NAC Sessions テーブルにあるフィールドの説明を示します。

表 30-16　show vpn-sessiondb summary コマンド：Active NAC Sessions および Total Cumulative NAC Sessions のフィールド

フィールド	説明
Accepted	ポスチャ検証が成功し、Access Control Server によってアクセス ポリシーが付与されたピアの数。
Exempted	セキュリティ アプライアンス上に設定されたポスチャ検証免除リストのエントリに一致しているため、ポスチャ検証の対象とならないピアの数。
Hold-off	セキュリティ アプライアンスがポスチャ検証に成功した後、EAPoUDP 通信が途絶えたピアの数。このタイプのイベントが発生してから各ピアに対して次にポスチャ検証が試行されるまでの遅延は、NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）によって決まります。
N/A	VPN NAC グループ ポリシーに従って NAC がディセーブルになっているピアの数。

表 30-16　show vpn-sessiondb summary コマンド：Active NAC Sessions および Total Cumulative NAC Sessions のフィールド （続き）

フィールド	説明
Non-responsive	ポスチャ検証のための Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP 要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。セキュリティ アプライアンスのコンフィギュレーションがクライアントレス ホストをサポートする場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアのセキュリティ アプライアンスにダウンロードします。クライアントレス ホストをサポートしない場合、セキュリティ アプライアンスは NAC デフォルト ポリシーを割り当てます。
Rejected	ポスチャ検証に失敗したか、または Access Control Server によってアクセス ポリシーが付与されなかったピアの数。

Active VLAN Mapping Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative VLAN Mapping Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 30-17 に、Active VLAN Mapping Sessions テーブルおよび Cumulative VLAN Mapping Sessions テーブルにあるフィールドの説明を示します。

表 30-17　show vpn-sessiondb summary コマンド：Active VLAN Mapping Sessions および Cumulative Active VLAN Mapping Sessions のフィールド

フィールド	説明
Access	将来的な使用のために予約されています。
Auth	将来的な使用のために予約されています。
Guest	将来的な使用のために予約されています。
N/A	将来的な使用のために予約されています。
Quarantine	将来的な使用のために予約されています。
Static	このフィールドには、事前設定された VLAN に割り当てられている VPN セッションの数が表示されます。

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show wccp

Web Cache Communication Protocol（WCCP）に関連するグローバル統計情報を表示するには、特権 EXEC モードで **show wccp** コマンドを使用します。

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

構文の説明

web-cache	Web キャッシュ サービスの統計情報を指定します。
service-number	（任意）キャッシュが制御する Web キャッシュ サービス グループの ID 番号。指定できる番号の範囲は 0 ～ 256 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。
detail	（任意）ルータおよびすべての Web キャッシュに関する情報を表示します。
view	（任意）特定のサービス グループの他のメンバーが検出されたかどうかを表示します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、WCCP 情報を表示する例を示します。

```
hostname(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
```

```
        Total Bypassed Packets Received:     0
hostname(config)#
```

関連コマンド

コマンド	説明
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

show webvpn csd

CSD がイネーブルかどうかを判定し、イネーブルの場合は実行コンフィギュレーションの CSD バージョンを表示したり、ファイルをテストして有効な CSD 配布パッケージかどうかを確認したりするには、特権 EXEC モードで **show webvpn csd** コマンドを使用します。

show webvpn csd [**image** *filename*]

構文の説明

filename	CSD 配布パッケージとしての有効性をテストするファイルの名前を指定します。この名前は、必ず securedesktop_asa_<*n*>_<*n*>*.pkg の形式とします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

CSD の動作ステータスを確認するには、**show webvpn csd** コマンドを使用します。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `Secure Desktop is not enabled.`

  CSD は実行コンフィギュレーション内にありますが、ディセーブルにされています。CSD をイネーブルにするには、webvpn コンフィギュレーション モードを開始して **csd enable** コマンドを入力します。

- `Secure Desktop version n.n.n.n is currently installed and enabled.`

  CSD はイネーブルに設定されています。バージョン番号は、フラッシュ デバイスから読み込まれる配布パッケージによって決まります。Cisco Secure Desktop Manager には、[ASDM Configuration] > [CSD] のメニュー パスからアクセスできます。ユーザが CSD にアクセスできるのは、CSD コンフィギュレーションに場所が含まれている場合だけです。

ファイルをテストして有効な CSD 配布パッケージかどうかを確認するには、**show webvpn csd image** コマンドを使用します。同様に、webvpn コンフィギュレーション モードで **csd image** コマンドを入力した場合は、コマンドで指定したファイルが有効な CSD 配布パッケージである場合にのみ、CSD がインストールされます。無効なパッケージの場合は、「ERROR: Unable to use CSD image」というメッセージが表示されます。

show webvpn csd image コマンドでファイルをテストして、有効な CSD 配布パッケージかどうかを確認しますが、ファイルが有効な場合でも CSD が自動的にインストールされることはありません。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `ERROR: This is not a valid Secure Desktop image file.`

  ファイル名が securedesktop_asa_<*n*>_<n>*.pkg の形式になっていることを確認します。ファイル名の形式が正しい場合は、次の Web サイトから取得した新しいファイルに置き換えます。

  http://www.cisco.com/cisco/software/navigator.html

  次に、**show webvpn csd image** コマンドを再入力します。イメージが有効な場合は、webvpn コンフィギュレーション モードで **csd image** コマンドおよび **csd enable** コマンドを使用し、CSD をインストールしてイネーブルにします。

- This is a valid Cisco Secure Desktop image:
  Version : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

  ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

例

次に、CSD が実行コンフィギュレーションにインストールされ、イネーブルにされた例を示します。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname#
```

次に、指定したファイルが有効な CSD イメージである例を示します。

```
hostname#show webvpn csd image securedesktop_asa_3_1_0_25.pkg

This is a valid Cisco Secure Desktop image:
  Version  : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

hostname#
```

関連コマンド

コマンド	説明
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

show webvpn group-alias

特定のトンネル グループまたはすべてのトンネル グループのエイリアスを表示するには、特権 EXEC モードで **group-alias** コマンドを使用します。

show webvpn group-alias [*tunnel-group*]

構文の説明

tunnel-group	（任意）グループ エイリアスを表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべてのエイリアスが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

使用上のガイドライン

show webvpn group-alias コマンドを入力する場合は、WebVPN が実行されている必要があります。

各トンネル グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。

例

次に、トンネル グループ「devtest」のエイリアスを表示する **show webvpn group-alias** コマンドと、このコマンドの出力例を示します。

```
hostname# show webvpn group-alias devtest
QA
Fra-QA
```

関連コマンド

コマンド	説明
group-alias	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn group-url

特定のトンネル グループまたはすべてのトンネル グループの URL を表示するには、特権 EXEC モードで **group-url** コマンドを使用します。

show webvpn group-url [*tunnel-group*]

構文の説明

tunnel-group	（任意）URL を表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべての URL が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

show webvpn group-url コマンドを入力する場合は、WebVPN が実行されている必要があります。各グループには複数の URL があることも、URL がまったくないこともあります。

例

次に、トンネル グループ「frn-eng1」の URL を表示する **show webvpn group-url** コマンドと、このコマンドの出力例を示します。

```
hostname# show webvpn group-url
http://www.cisco.com
https://fra1.vpn.com
https://fra2.vpn.com
```

関連コマンド

コマンド	説明
group-url	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn sso-server

WebVPN シングル サインオン サーバに関する運用統計情報を表示するには、特権 EXEC モードで **show webvpn sso-server** コマンドを使用します。

show webvpn sso-server [*name*]

構文の説明

name	（任意）SSO サーバの名前を指定します。サーバ名の長さは 4 ～ 31 文字にする必要があります。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**show webvpn sso-server** コマンドは、セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。

SSO サーバ名引数が入力されていない場合は、すべての SSO サーバの統計情報が表示されます。

例

次に、特権 EXEC モードでコマンドを入力し、タイプが SiteMinder、名前が example である SSO サーバの統計情報を表示する例を示します。

```
hostname# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
```

```
Number of unrecognized responses:  0
hostname#
```

次に、特定の SSO サーバ名を指定せずにこのコマンドを発行することで、セキュリティ アプライアンスで設定されているすべての SSO サーバに関する統計情報を表示する例を示します。

```
hostname#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
asa1(config-webvpn)#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

show webvpn svc

セキュリティ アプライアンスにインストールされ、キャッシュ メモリに読み込まれる SSL VPN クライアント イメージについての情報を表示するには、またはファイルが有効なクライアント イメージであるかテストするには、特権 EXEC モードで **show webvpn svc** コマンドを使用します。

show webvpn svc [**image** *filename*]

構文の説明

image *filename*	SSL VPN クライアント イメージ ファイルとしてテストするファイルの名前を指定します。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシュ メモリにロードされ、リモート PC にダウンロード可能な SSL VPN クライアント イメージに関する情報を表示するには、**show webvpn svc** コマンドを使用します。ファイルをテストして有効なイメージかどうかを確認するには、**image** *filename* のキーワードと引数を使用します。ファイルが有効なイメージではない場合、次のメッセージが表示されます。

```
ERROR: This is not a valid SSL VPN Client image file.
```

例

次に、現在インストールされているイメージに対する **show webvpn svc** コマンドの出力例を示します。

```
hostname# show webvpn svc
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

次に、有効なイメージに対する **show webvpn svc image** *filename* コマンドの出力例を示します。

```
F1(config-webvpn)# show webvpn svc image sslclient-win-1.0.2.127.pkg
```

```
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

関連コマンド

コマンド	説明
svc enable	セキュリティ アプライアンスで SSL VPN クライアントをリモート PC にダウンロードできるようにします。
svc image	セキュリティ アプライアンスがフラッシュ メモリからキャッシュメモリに SSL VPN クライアント ファイルをロードするようにします。クライアント イメージをオペレーティング システムと照合するときに、セキュリティ アプライアンスがクライアント イメージの各部分をリモート PC にダウンロードする順序を指定します。
vpn-tunnel-protocol	SSL VPN クライアントが使用する SSL を含め、リモート VPN ユーザの特定の VPN トンネル プロトコルをイネーブルにします。

show xlate

変換スロットに関する情報を表示するには、特権 EXEC モードで **show xlate** コマンドを使用します。

show xlate [**global** *ip1*[*-ip2*] [**netmask** *mask*]] [**local** *ip1*[*-ip2*] [**netmask** *mask*]]
[**gport** *port1*[*-port2*]] [**lport** *port1*[*-port2*]] [**interface** *if_name*] [**state** *state*] [**debug**] [**detail**]

show xlate count

構文の説明

count	変換数を表示します。
debug	（任意）xlate のデバッグ情報を表示します。
detail	（任意）xlate の詳細情報を表示します。
global *ip1*[*-ip2*]	（任意）グローバル IP アドレスまたはアドレス範囲を指定して、アクティブな変換を表示します。
gport *port1*[*-port2*]	グローバル ポートまたはポート範囲を指定して、アクティブな変換を表示します。
interface *if_name*	（任意）アクティブな変換をインターフェイス別に表示します。
local *ip1*[*-ip2*]	（任意）ローカル IP アドレスまたはアドレス範囲を指定して、アクティブな変換を表示します。
lport *port1*[*-port2*]	ローカル ポートまたはポート範囲を指定して、アクティブな変換を表示します。
netmask *mask*	（任意）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（任意）状態を指定して、アクティブな変換を表示します。次の 1 つ以上の状態を入力できます。 • **static**：スタティック変換を指定します。 • **portmap**：PAT グローバル変換を指定します。 • **norandomseq**：**norondomseq** 設定での **nat** またはスタティック変換を指定します。 • **identity**：**nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ってください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show xlate コマンドは、変換スロットの内容を表示します。**show xlate detail** コマンドは、次の情報を表示します。

- {**ICMP**|**TCP**|**UDP**} **PAT from** *interface*:*real-address*/*real-port* **to** *interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*
- **NAT from** *interface*:*real-address*/*real-port to interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*

表 30-18 に、変換フラグの定義を示します。

表 30-18　変換フラグ

フラグ	説明
s	スタティック変換スロット
d	次のクリーニング サイクルのダンプ変換スロット
r	ポート マップ変換（ポート アドレス変換）
n	TCP シーケンス番号の非ランダム化
i	内部アドレス変換
D	DNS A RR リライト
I	**nat 0** からの ID 変換

（注） **vpnclient** コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合に **show xlate** コマンドを実行すると、1 つのスタティック変換に対応する複数の xlate が表示されることがあります。

例

次に、**show xlate** コマンドの出力例を示します。3 つのアクティブな PAT とともに変換スロット情報が表示されています。

```
hostname# show xlate

3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

次に、**show xlate detail** コマンドの出力例を示します。3 つのアクティブな PAT とともに、変換タイプおよびインターフェイス情報が表示されています。

最初のエントリは、内部ネットワークのホスト ポート（10.1.1.15、1025）から外部ネットワークのホスト ポート（192.150.49.1、1024）への TCP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレス ポートに適用されることを示しています。

2 番めのエントリは、内部ネットワークのホスト ポート（10.1.1.15、1028）から外部ネットワークのホスト ポート（192.150.49.1、1024）への UDP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレス ポートに適用されることを示しています。

3 番めのエントリは、内部ネットワークのホスト ICMP ID（10.1.1.15、21505）から外部ネットワークのホスト ICMP ID（192.150.49.1、0）への ICMP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレス ICMP ID に適用されることを示します。

セキュリティが高いインターフェイスから低いインターフェイスに移動するパケットの場合、内部アドレス フィールドは送信元アドレスとして表示されます。セキュリティが低いインターフェイスから高いインターフェイスに移動するパケットでは、宛先アドレスとして表示されます。

```
hostname# show xlate detail

3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

次に、**show xlate** コマンドの出力例を示します。2 つのスタティック変換が表示されています。最初の変換には 1 つの接続（「nconns」）が関連付けられ、2 番めの変換には 4 つの接続が関連付けられています。

```
hostname# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

関連コマンド

コマンド	説明
clear xlate	現在の変換および接続情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show uauth	現在認証済みのユーザを表示します。

CHAPTER 31

shun コマンド～ sysopt radius ignore-secret コマンド

shun

攻撃元ホストからの接続をブロックするには、特権 EXEC モードで **shun** コマンドを使用します。shun をディセーブルにするには、このコマンドの **no** 形式を使用します。

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

構文の説明

dest_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。
dest_ip	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。
protocol	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。
source_ip	攻撃元ホストのアドレスを指定します。送信元 IP アドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。
source_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。
vlan_id	（任意）送信元ホストが配置されている VLAN ID を指定します。

デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続をブロックできます。送信元 IP アドレスからの今後のすべての接続は、手動または Cisco IPS センサーによってブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。**shun** コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

shun コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

shun コマンドは攻撃をダイナミックにブロックするために使用されるため、セキュリティ アプライアンス コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。新しいインターフェイスを追加するか、または同じインターフェイスを（同じ名前を使用して）置き換える場合、IPS センサーでそのインターフェイスをモニタするには、そのインターフェイスを IPS センサーに追加する必要があります。

例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、セキュリティ アプライアンス接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、**shun** コマンドを適用します。

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドにより、現在の接続はセキュリティ アプライアンス接続テーブルから削除され、10.1.1.27 からの今後のすべてのパケットはセキュリティ アプライアンスを通過できなくなります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
show conn	すべてのアクティブな接続を表示します。
show shun	回避についての情報を表示します。

shutdown

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

すべての物理インターフェイスは、デフォルトではシャットダウンされます。セキュリティ コンテキスト内の割り当て済みのインターフェイスは、コンフィギュレーション内でシャットダウンされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

（注）　このコマンドでは、ソフトウェア インターフェイスのみがディセーブルになります。物理リンクはアップのまま維持され、対応するインターフェイスが **shutdown** コマンドを使用して設定された場合でも、直接接続されたデバイスはアップであると認識されます。

例

次に、メイン インターフェイスをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次に、サブインターフェイスをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、サブインターフェイスをシャットダウンする例を示します。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

shutdown（ca-server モード）

ローカル Certificate Authority（CA; 認証局）サーバをディセーブルにし、ユーザが登録インターフェイスにアクセスできないようにするには、CA サーバ コンフィギュレーション モードで **shutdown** コマンドを使用します。CA サーバをイネーブルにし、コンフィギュレーションをロックして変更できないようにし、登録インターフェイスにアクセスできるようにするには、このコマンドの **no** 形式を使用します。

[no] shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

最初は、CA サーバはデフォルトでシャットダウンされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CA サーバ モードのこのコマンドは、インターフェイス モードの **shutdown** コマンドと類似しています。セットアップ時に、ローカル CA サーバはデフォルトでシャットダウンされるため、**no shutdown** コマンドを使用してイネーブルにする必要があります。**no shutdown** コマンドを初めて使用するときは、CA サーバをイネーブルにし、CA サーバ証明書とキー ペアを生成します。

（注） **no shutdown** コマンドを発行することによって、CA コンフィギュレーションをロックして CA 証明書を生成した後は、CA コンフィギュレーションを変更できません。

no shutdown コマンドで CA サーバをイネーブルにして現在のコンフィギュレーションをロックするには、生成される CA 証明書とキー ペアが含まれる PKCS12 ファイルを符号化してアーカイブするために、7 文字のパスワードが必要です。このファイルは、以前に指定した **database path** コマンドで識別されるストレージに格納されます。

例

次に、ローカル CA サーバをディセーブルにし、登録インターフェイスにアクセスできないようにする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# shutdown
```

```
hostname(config-ca-server)#
```

次に、ローカル CA サーバをイネーブルにし、登録インターフェイスにアクセスできるようにする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no shutdown
hostname(config-ca-server)#

hostname(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

sla monitor

SLA 動作を作成するには、グローバル コンフィギュレーション モードで **sla monitor** コマンドを使用します。SLA 動作を削除するには、このコマンドの **no** 形式を使用します。

sla monitor *sla_id*

no sla monitor *sla_id*

構文の説明

sla_id	設定する SLA の ID を指定します。SLA が存在しない場合は、作成されます。有効な値は 1 ～ 2147483647 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

sla monitor コマンドによって、SLA 動作が作成され、SLA モニタ コンフィギュレーション モードが開始されます。このコマンドを入力すると、コマンド プロンプトは `hostname(config-sla-monitor)#` に変わり、SLA モニタ コンフィギュレーション モードになったことが示されます。SLA 動作がすでに存在し、それに対してタイプがすでに定義されている場合、プロンプトは `hostname(config-sla-monitor-echo)#` と表示されます。最大 2000 個の SLA 動作を作成できます。任意の時点でデバッグできるのは 32 個の SLA 動作のみです。

no sla monitor コマンドによって、指定した SLA 動作およびその動作を設定するために使用されたコマンドが削除されます。

SLA 動作を設定した後、**sla monitor schedule** コマンドで動作をスケジューリングする必要があります。スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

動作の現在のコンフィギュレーション設定を表示するには、**show sla monitor configuration** コマンドを使用します。SLA 動作の動作統計情報を表示するには、**show sla monitor operation-state** コマンドを使用します。コンフィギュレーション内の SLA コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor schedule	SLA 動作をスケジューリングします。
timeout	SLA 動作が応答を待機する時間を設定します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

sla monitor schedule

SLA 動作をスケジューリングするには、グローバル コンフィギュレーション モードで **sla monitor schedule** コマンドを使用します。SLA 動作のスケジュールを削除し、動作を保留状態にするには、このコマンドの **no** 形式を使用します。

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

構文の説明

after *hh*:*mm*:*ss*	コマンドの入力後、何時間、何分、何秒で動作が開始されるかを示します。
ageout *seconds*	（任意）情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で指定します。エージング アウト後、SLA 動作は実行コンフィギュレーションから削除されます。
day	動作を開始する日。有効な値は、1 ～ 31 です。日を指定しない場合、現在の日が使用されます。日を指定する場合は、月も指定する必要があります。
hh:*mm*[:*ss*]	絶対開始時刻を 24 時間表記で指定します。秒は任意です。*month* および *day* を指定しない場合は、指定した時刻が次に来たときとなります。
life forever	（任意）無期限に実行されるように動作をスケジューリングします。
life *seconds*	（任意）動作によって情報がアクティブに収集される秒数を設定します。
month	（任意）動作を開始する月の名前。月を指定しない場合、現在の月が使用されます。月を指定する場合は、日も指定する必要があります。 月の英語名を完全に入力するか、または、最初の 3 文字のみを入力します。
now	コマンドを入力するとすぐに動作が開始されることを示します。
pending	情報が収集されないことを示します。これは、デフォルトの状態です。
recurring	（任意）動作が毎日、指定した時刻に自動的に開始され、指定した時間継続されることを示します。
sla-id	スケジューリングする SLA 動作の ID。
start-time	SLA 動作が開始される時刻を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- SLA 動作は、スケジューリングされた時間になるまで **pending** 状態です。つまり、動作はイネーブルですが、データはアクティブに収集されていません。
- デフォルトの **ageout** 時間は、0 秒（エージング アウトしない）です。
- デフォルトの **life** は、3600 秒（1 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA 動作がアクティブ状態の場合、ただちに情報の収集が開始されます。次のタイム ラインは、動作のエージング アウト プロセスを示しています。

```
W----------------------X----------------------Y----------------------Z
```

- W は、SLA 動作が **sla monitor** コマンドで設定された時刻です。
- X は、SLA 動作の開始時刻です。これは、動作が「アクティブ」になったときです。
- Y は、**sla monitor schedule** コマンドで設定された有効期間の終了です（**life** の秒数は 0 までカウント減少されました）。
- Z は、動作のエージング アウトです。

エージング アウト プロセスが使用される場合、エージング アウト プロセスは、W でカウントダウンを開始し、X と Y の間は中断され、Y で設定されたサイズにリセットされてカウントダウンを再開します。SLA 動作がエージング アウトすると、SLA 動作のコンフィギュレーションは実行コンフィギュレーションから削除されます。動作は、実行される前にエージング アウトする可能性があります（つまり、Z が X の前に発生する可能性があります）。このような状況が発生しないようにするには、動作のコンフィギュレーション時刻と開始時刻（X と W）の差を、エージング アウトの秒数よりも小さくする必要があります。

recurring キーワードは、単一の SLA 動作のスケジューリングに対してのみサポートされています。1 つの **sla monitor schedule** コマンドを使用して複数の SLA 動作をスケジューリングすることはできません。定期的な SLA 動作の **life** 値は、1 日未満にする必要があります。定期的な動作の **ageout** 値を「なし」（値 0 で指定）にするか、**life** 値と **ageout** 値の合計を 1 日よりも大きくする必要があります。recurring オプションを指定しないと、動作は既存の通常のスケジューリング モードで開始されます。

スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

例

次に、4 月 5 日午後 3 時にデータの収集をアクティブに開始するようにスケジューリングされた SLA 動作 25 の例を 示します。この動作は、非アクティブになって 12 時間後にエージング アウトします。この SLA 動作がエージング アウトすると、SLA 動作のすべてのコンフィギュレーション情報は実行コンフィギュレーションから削除されます。

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

次に、5 分間の遅延の後にデータの収集を開始するようにスケジューリングされた SLA 動作 1 の例を示します。デフォルトの有効期間である 1 時間が適用されます。

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

次に、ただちにデータの収集を開始するようにスケジューリングされた SLA 動作 3 の例を示します。この例は、無期限に実行されるようにスケジューリングされています。

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

次に、毎日午前 1 時 30 分にデータの収集を自動的に開始するようにスケジューリングされた SLA 動作 15 の例を示します。

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

関連コマンド

コマンド	説明
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor	SLA モニタリング動作を定義します。

smart-tunnel auto-signon enable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル自動サインオンをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-signon enable** コマンドを使用します。

[**no**] **smart-tunnel auto-signon enable** *list* [**domain** *domain*]

グループ ポリシーまたはユーザ名から **smart-tunnel auto-signon enable** コマンドを削除し、デフォルトのグループ ポリシーから継承するには、このコマンドの **no** 形式を使用します。

構文の説明

list	*list* は、セキュリティ アプライアンスの webvpn コンフィギュレーションにすでに存在するスマート トンネル自動サインオン リストの名前です。 SSL VPN コンフィギュレーション内のスマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。
domain *domain*	（任意）認証中にユーザ名に追加されるドメインの名前。ドメインを入力する場合、**use-domain** キーワードをリスト エントリに入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

smart-tunnel auto-signon *list* コマンドを使用して、最初にサーバのリストを作成する必要があります。グループ ポリシーまたはユーザ名に割り当てることができるリストは 1 つだけです。

例

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR
hostname(config-group-webvpn)
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザ名に追加します。

```
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

```
hostname(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon *list*	スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成します。
show running-config webvpn smart-tunnel	セキュリティ アプライアンスのスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel *list*	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel auto-signon list

スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel auto-signon list** コマンドを使用します。

[**no**] **smart-tunnel auto-signon** *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

リストに追加する各サーバに対してこのコマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。リストと、セキュリティ アプライアンス コンフィギュレーションに表示されている IP アドレスまたはホスト名を指定します。スマート トンネル自動サインオン リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

サーバのリスト全体をセキュリティ アプライアンス コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストのみを指定します。

no smart-tunnel auto-signon *list*

構文の説明

host	ホスト名またはワイルドカード マスクによって識別されるサーバ。
hostname-mask	自動認証する対象のホスト名またはワイルドカード マスク。
ip	IP アドレスおよびネット マスクによって識別されるサーバ。
ip-address [*netmask*]	自動認証する対象のホストのサブネットワーク。
list	リモート サーバのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合は、セキュリティ アプライアンスによって作成されます。存在する場合、リストにエントリを追加します。
use-domain	（任意）認証で必要な場合、Windows ドメインをユーザ名に追加します。このキーワードを入力する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーまたはユーザ名に割り当てるときにドメイン名を指定してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。

スマート トンネル自動サインオン リストの入力に続き、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **smart-tunnel auto-signon enable** *list* コマンドを使用してリストを割り当てます。

例

次のコマンドでは、サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザ名に追加します。

```
asa2(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0
```

次のコマンドは、リストからエントリを削除します。

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

前述のコマンドでは、削除されるエントリがリストの唯一のエントリである場合、HR という名前のリストも削除されます。唯一のエントリではない場合は、次のコマンドによってリスト全体がセキュリティ アプライアンス コンフィギュレーションから削除されます。

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR
```

次のコマンドでは、ドメイン内のすべてのホストを intranet という名前のスマート トンネル自動サインオン リストに追加します。

```
asa2(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

次のコマンドは、リストからエントリを削除します。

```
asa2(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon enable	コマンド モードで指定されたグループ ポリシーまたはユーザ名に対して、スマート トンネル自動サインオンをイネーブルにします。
smart-tunnel auto-signon enable *list*	グループ ポリシーまたはユーザ名にスマート トンネル自動サインオン リストを割り当てます。
show running-config webvpn smart-tunnel	スマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smart-tunnel auto-start

クライアントレス（ブラウザベース）SSL VPN セッションでユーザがログインしたときにスマート トンネル アクセスを自動的に開始するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-start** コマンドを使用します。

smart-tunnel auto-start *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、セキュリティ アプライアンス webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内にすでに存在するスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のアプリケーションのリストについて、スマート トンネル アクセスを開始します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
hostname(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル コマンドを継承します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel disable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル アクセスを禁止するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel disable** コマンドを使用します。

smart-tunnel disable

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除して、デフォルトのグループ ポリシーから [**no**] **smart-tunnel** コマンドを継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトではスマート トンネルはイネーブルではないため、**smart-tunnel disable** コマンドは（デフォルトの）グループ ポリシーまたはユーザ名コンフィギュレーションに、対象のポリシーまたはユーザ名に適用しない **smart-tunnel auto-start** または **smart-tunnel enable** コマンドが含まれている場合にのみ必要です。

例

次のコマンドでは、スマート トンネル アクセスを禁止します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel disable
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
`smart-tunnel auto-start`	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
`smart-tunnel enable`	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。
`smart-tunnel list`	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel enable

クライアントレス（ブラウザベース）SSL VPN セッションでスマート トンネル アクセスをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**smart-tunnel enable** コマンドを使用します。

smart-tunnel enable *list*

グループ ポリシーまたはユーザ名から **smart-tunnel** コマンドを削除し、デフォルト グループ ポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list	*list* は、セキュリティ アプライアンス webvpn コンフィギュレーションにすでに存在するスマート トンネル リストの名前です。 SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

smart-tunnel enable コマンドによって、スマート トンネル アクセスに適格なアプリケーションのリストがグループ ポリシーまたはユーザ名に割り当てられます。ユーザは、クライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。または、**smart-tunnel auto-start** コマンドを使用して、ユーザがログインしたときに自動的にスマート トンネル アクセスを開始できます。

いずれのコマンドでも、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストをイネーブルにします。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
hostname(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル リストを継承します。

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel list

プライベート サイトに接続する場合にクライアントレス（ブラウザベース）SSL VPN セッションを使用できるアプリケーションのリストに入力するには、webvpn コンフィギュレーション モードで **smart-tunnel list** コマンドを使用します。

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

アプリケーションをリストから削除するには、このコマンドの **no** 形式を使用して、エントリを指定します。アプリケーションのリスト全体をセキュリティ アプライアンス コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストだけを指定します。

no smart-tunnel list *list*

構文の説明

list	アプリケーションまたはプログラムのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。コンフィギュレーション内にリストが存在しない場合は、CLI によって作成されます。存在する場合、リストにエントリを追加します。
application	スマート トンネル アクセスが付与されるアプリケーションの名前。文字列は最大 64 文字まで使用できます。
path	Mac OS の場合は、アプリケーションのフル パス。Windows の場合は、アプリケーションのファイル名。または、ファイル名を含むアプリケーションのフル パスまたは部分パス。ストリングには最大 128 文字を使用できます。
platform *OS*	（OS が Microsoft Windows の場合は任意）**windows** または **mac** を入力して、アプリケーションのホストを指定します。
hash	（任意。Windows にのみ該当）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft File Checksum Integrity Verifier（FCIV; ファイル チェックサム整合性検証）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。 SHA-1 ハッシュは、常に 16 進数 40 文字です。

デフォルト

Windows がデフォルトのプラットフォームです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**platform** *OS* が追加されました。

使用上のガイドライン

複数のスマート トンネル リストをセキュリティ アプライアンスで設定できますが、複数のスマート トンネル リストを特定のグループ ポリシーまたはユーザ名に割り当てることはできません。スマート トンネル リストに入力するには、アプリケーションごとに **smart-tunnel list** コマンドを 1 回入力します。同じ *list* ストリングを入力しますが、OS で一意の *application* および *path* を指定します。リストでサポートする各 *OS* について、コマンドを 1 回入力します。

OS がエントリで指定されたものと一致しない場合、セッションでリスト エントリは無視されます。アプリケーションのパスが存在しない場合も、エントリは無視されます。

SSL VPN コンフィギュレーション内のスマート トンネル リストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

path はコンピュータ上のものと一致する必要がありますが、完全である必要はありません。たとえば、実行ファイルとその拡張子だけで *path* を構成できます。

スマート トンネルには次の要件があります。

- スマート トンネル接続を開始するリモート ホストでは、32 ビット バージョンの Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 が実行されている必要があります。
- スマート トンネルまたはポート フォワーディングを使用する Microsoft Windows Vista のユーザは、ASA の URL を [Trusted Site] ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動して、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザは、[Protected Mode] をディセーブルにしてスマート トンネル アクセスを容易にすることもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法は推奨しません。
- ブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- Mac OS のスマート トンネル サポートには、Safari 3.1.1 以降が必要です。

Microsoft Windows では、Winsock 2、TCP ベースのアプリケーションのみがスマート トンネル アクセスに適格です。

Mac OS では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できます。次のタイプのアプリケーションは、スマート トンネルで使用できません。

- dlopen または dlsym を使用して libsocket コールを特定するアプリケーション
- libsocket コールを特定するためにスタティックにリンクされたアプリケーション
- 2 レベルのネーム スペースを使用する Mac OS アプリケーション
- Mac OS のコンソールベースのアプリケーション（Telnet、SSH、cURL など）
- PowerPC MAC オペレーティング システムはスマート トンネルではサポートされません。

Mac OS では、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できます。この要件には、Firefox のスマート トンネル サポートが含まれています。スマート トンネルの最初の使用中に Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザ プロファイルが必要です。このユーザ プロファイルが存在しない場合、セッションでは、作成するようにユーザに要求します。

次の制限事項がスマート トンネルに適用されます。

- リモート コンピュータがセキュリティ アプライアンスにアクセスするためにプロキシ サーバを必要とする場合、接続の終端側の URL が、プロキシ サービスから除外される URL のリストに存在する必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。
- セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。スマート トンネル機能もポート フォワーディングも MAPI をサポートしていません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。
- スマート トンネル自動サインオン機能では、Microsoft Windows OS 上の Microsoft WININET ライブラリを使用して HTTP または HTTPS 通信を行うアプリケーションのみがサポートされます。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバと通信します。
- グループ ポリシーまたはローカル ユーザ ポリシーでは、スマート トンネル アクセスに適格なアプリケーションのリスト 1 つと、スマート トンネル自動サインオン サーバのリスト 1 つだけがサポートされます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザはフェールオーバー後に再接続する必要があります。

（注） スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*path* 値が最新でないことを示している場合があります。たとえば、アプリケーションおよび次のアップグレードを作成する会社が買収されると、アプリケーションのデフォルトのパスは通常は変更されます。

ハッシュを入力すると、*path* で指定したストリングと一致する不適格なファイルがクライアントレス SSL VPN によって認定されないことが、ある程度保証されます。チェックサムはアプリケーションの各バージョンまたはパッチによって異なるため、入力する *hash* が一致するのは、リモート ホスト上の 1 つのバージョンまたはパッチのみです。アプリケーションの複数のバージョンに対して *hash* を指定するには、各バージョンに対して **smart-tunnel list** コマンドを 1 回入力します。このとき、各コマンドでは、同じ *list* ストリングを入力しますが、一意の *application* ストリングと一意の *hash* 値を指定します。

（注） *hash* 値を入力し、スマート トンネル アクセスでアプリケーションの今後のバージョンまたはパッチをサポートする場合は、今後もスマート トンネル リストを維持する必要があります。スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*hash* 値を含むアプリケーション リストが最新でないことを示している場合があります。この問題は *hash* を入力しないことによって回避できます。

スマート トンネル リストのコンフィギュレーションに続き、**smart-tunnel auto-start** または **smart-tunnel enable** コマンドを使用して、グループ ポリシーまたはユーザ名にリストを割り当てます。

例

次のコマンドでは、connect.exe という名前の Microsoft Windows アプリケーションを apps1 という名前のスマート トンネル リストに追加します。

```
hostname(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

次のコマンドでは、Windows アプリケーション msimn.exe を追加し、リモート ホスト上のアプリケーションのハッシュが、スマート トンネル アクセスを許可するために入力された最後のストリングと一致することを要求します。

```
hostname(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

次のコマンドでは、Mac OS ブラウザ Safari にスマート トンネル サポートを提供します。

```
hostname(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

関連コマンド

コマンド	説明
show running-config webvpn smart-tunnel	セキュリティ アプライアンスのスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザ ログイン時にスマート トンネル アクセスをイネーブルにします。ただし、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access] > [Start Smart Tunnels] ボタンを使用して、手動でスマート トンネル アクセスを開始する必要があります。

smartcard-removal-disconnect

スマート カードがユーザのコンピュータから取り外された場合に IPSec クライアント セッションを切断または保持するには、グループ ポリシー コンフィギュレーション モードで **smartcard-removal-disconnect** コマンドを使用します。

smartcard-removal-disconnect {**enable** | **disable**}

グループ ポリシーから **smartcard-removal-disconnect** コマンドを削除し、デフォルトのグループ ポリシーから設定を継承するには、このコマンドの **no** 形式を使用します。

no smartcard-removal-disconnect

構文の説明

enable	スマート カードがユーザのコンピュータから取り外された場合に IPSec クライアント セッションを終了します。
disable	スマート カードがユーザのコンピュータから取り外されても IPSec クライアント セッションを続行します。

デフォルト

enable

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、認証に使用されるスマート カードが取り外された場合に IPSec クライアント セッションは切断されます。接続中にスマート カードをコンピュータに入れたままにする必要がないようにする場合は、**smartcard-removal-disconnect disable** コマンドを入力します。

例

次のコマンドでは、スマート カードがユーザのコンピュータから取り外されてもクライアント セッションが続行するようにします。

```
hostname(config-group-policy)# smartcard-removal-disconnect disable
hostname(config-group-policy)
```

次のコマンドでは、スマート カードがユーザのコンピュータから取り外された場合にクライアント セッションが終了されるようにします。

```
hostname(config-group-policy)# smartcard-removal-disconnect enable
```

smtp from-address

ローカル CA サーバが生成するすべての電子メール（ワンタイム パスワードの配布など）の送信者フィールドで使用する電子メール アドレスを指定するには、CA サーバ コンフィギュレーション モードで **smtp from-address** コマンドを使用します。電子メール アドレスをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp from-address *e-mail_address*

no smtp from-address

構文の説明

e-mail_address	CA サーバが生成するすべての電子メールの送信者フィールドに表示する電子メール アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドに ca-admin@asa1-ca.example.com が含まれるように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
hostname(config-ca-server)#
```

次に、ローカル CA サーバからの、すべての電子メールの送信者フィールドをデフォルトのアドレス admin@asa1-ca.example.com にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address admin@asa1-ca.example.com
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。

smtp subject

ローカル Certificate Authority（CA; 認証局）サーバが生成するすべての電子メール（ワンタイム パスワードの配布など）の件名フィールドに表示するテキストをカスタマイズするには、CA サーバ コンフィギュレーション モードで **smtp subject** コマンドを使用します。テキストをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

smtp subject *subject-line*

no smtp subject

構文の説明

subject-line	CA サーバから送信するすべての電子メールの件名フィールドに表示するテキストを指定します。最大文字数は 127 です。

デフォルト

デフォルトでは、件名フィールドのテキストは「Certificate Enrollment Invitation」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、CA サーバからの、すべての電子メールの件名フィールドにテキスト *Action: Enroll for a certificate* を表示するように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp subject Action: Enroll for a certificate
hostname(config-ca-server)#
```

次に、CA サーバからの、すべての電子メールの件名フィールドのテキストをデフォルトのテキスト「Certificate Enrollment Invitation」にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no smtp subject
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
smtp from-address	ローカル CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。

smtps

SMTPS コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンド モードで入力されたコマンドを削除するには、このコマンドの **no** 形式を使用します。SMTPS は、SSL 接続での電子メールの送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、SMTPS コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# smtps
hostname(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバを設定するには、グローバル コンフィギュレーション モードで **smtp-server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

セキュリティ アプライアンスには、内部 SMTP クライアントが含まれており、特定のイベントが発生したことを外部エンティティに通知するためにイベント システムで使用できます。これらのイベント通知を受信し、指定された電子メール アドレスに転送するように SMTP サーバを設定できます。SMTP 機能がアクティブになるのは、セキュリティ アプライアンス で電子メール イベントがイネーブルな場合だけです。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

構文の説明

primary_server	プライマリ SMTP サーバを指定します。IP アドレスまたは DNS 名を使用します。
backup_server	プライマリ SMTP サーバを使用できない場合にイベント メッセージをリレーするバックアップ SMTP サーバを識別します。IP アドレスまたは DNS 名を使用します。

デフォルト

デフォルトでは、SMTP サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、SMTP サーバを IP アドレス 10.1.1.24 を使用して設定し、バックアップ SMTP サーバを IP アドレス 10.1.1.34 を使用して設定する例を示します。

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-map

SNMP インスペクションのパラメータを定義するための特定のマップを指定するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map *map_name*

no snmp-map *map_name*

構文の説明

map_name	SNMP マップ名です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

snmp-map コマンドを使用して、SNMP インスペクションのパラメータを定義するために使用する特定のマップを指定します。このコマンドを入力すると、SNMP マップ コンフィギュレーション モードが開始され、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップの定義後、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
```

```
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

snmp-server community

SNMP コミュニティ ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。コミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community *text*

no snmp-server community [*text*]

構文の説明

text	コミュニティ ストリングを設定します。

デフォルト

コミュニティ ストリングは **public** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理されるネットワーク ノード間の共有秘密です。セキュリティ アプライアンスは、キーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、サイトにコミュニティ ストリングを指定してから、ルータ、セキュリティ アプライアンス、および管理ステーションに同じストリングを設定できます。セキュリティ アプライアンスはこのストリングを使用し、無効なコミュニティ ストリングを持つ要求には応答しません。

例

次の例では、コミュニティ ストリングを wallawallabingbang に設定します。

```
hostname(config)# snmp-server community wallawallabingbang
```

関連コマンド

コマンド	説明
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server contact

SNMP サーバのコンタクト名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。SNMP のコンタクト名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*

no snmp-server contact [*text*]

構文の説明

text	コンタクト担当者またはセキュリティ アプライアンス システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例では、SNMP サーバの連絡先を Pat Johnson と設定します。

```
hostname(config)# snmp-server contact Pat Johnson
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable

セキュリティ アプライアンスで SNMP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable

no snmp-server enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

SNMP サーバはイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、SNMP トラップやその他の設定を行ったり、これらを再設定しなくても、SNMP を簡単にイネーブルまたはディセーブルにすることができます。

例

次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。

コマンド	説明
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable traps

セキュリティ アプライアンスの NMS へのトラップ送信をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。トラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

構文の説明

all	すべてのトラップをイネーブルにします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** のトラップは次のとおりです。 • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	IPSec トラップをイネーブルにします。**ipsec** のトラップは次のとおりです。 • **start** • **stop**
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。リモート アクセスのトラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップを有効にします。デフォルトでは、すべての SNMP トラップはイネーブルになっています。**snmp** のトラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	システム ログ メッセージのトラップをイネーブルにします。

デフォルト

デフォルトのコンフィギュレーションでは、すべての **snmp** トラップがイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。ただし、**clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル状態に戻ります。

このコマンドを入力し、トラップ タイプを指定しない場合、デフォルトは **syslog** です（デフォルトの **snmp** トラップは **syslog** トラップとともに引き続きイネーブルのままです）。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　機能タイプごとにこのコマンドを入力して、個々のトラップまたはトラップのセットをイネーブルにするか、**all** キーワードを入力してすべてのトラップをイネーブルにします。

NMS にトラップを送信するには、**logging history** コマンドを入力し、**logging enable** コマンドを使用してロギングをイネーブルにします。

例　次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server group

新しい SNMP グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

構文の説明

auth	暗号化を使用しないパケット認証を指定します。
group-name	グループの名前を指定します。
noauth	パケット認証を指定しません。
priv	暗号化されたパケット認証を指定します。
v3	グループが SNMP バージョン 3 セキュリティ モデルを使用することを指定します。このセキュリティ モデルは、サポートされているものの中で最もセキュアです。このバージョンでは、認証特性を明示的に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。バージョン 3 およびセキュリティ レベルも指定する必要があります。コミュニティ ストリングが内部的に設定されている場合、「public」という名前の 2 つのグループが自動的に作成されます。1 つはバージョン 1 セキュリティ モデル用、もう 1 つはバージョン 2c セキュリティ モデル用です。コミュニティ ストリングを削除すると、設定された両方のグループが自動的に削除されます。

（注） 特定のグループに属すように設定されるユーザは、グループと同じセキュリティ モデルを持つ必要があります。

例

次の例に、セキュリティ アプライアンスが SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server user	新しい SNMP ユーザを作成します。

snmp-server host

セキュリティ アプライアンスで SNMP を使用可能な NMS を指定するには、グローバル コンフィギュレーション モードで **snmp-server host** コマンドを使用します。NMS をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

構文の説明

0	（任意）暗号化されていない（クリア テキストの）コミュニティ ストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community	NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、または NMS からの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。暗号化フォーマットと非暗号化フォーマット（クリア テキスト）を使用できます。
hostname	SNMP 通知ホストを指定します。通常は NMS または SNMP マネージャです。
interface	NMS がセキュリティ アプライアンスとの通信に使用するインターフェイス名を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の送信元の NMS の IP アドレスを指定します。IPv4 アドレスのみをサポートしています。
poll	（任意）ホストはブラウズ（ポーリング）は可能だが、トラップは送信されないことを指定します。
port	NMS ホストの UDP ポート番号を設定します。
trap	（任意）トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。
udp-port	（任意）SNMP トラップはデフォルト以外のポートで NMS ホストに送信される必要があることを指定します。
version {**1** | **2c** | **3**}	（任意）トラップの送信に使用する SNMP 通知バージョンを、バージョン 1、2c、または 3 に設定します。

デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(5)	暗号化パスワードのサポートが追加されました。

使用上のガイドライン

最大 32 個の NMS を指定できます。現在使用中のポートで **snmp-server host** コマンドを設定すると、次のメッセージが表示されます。

警告　**The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定し、SNMP ホストを設定する必要があります。ユーザ名はデバイス上で設定済みである必要があります。デバイスがフェールオーバー ペアのスタンバイ ユニットとして設定される場合、SNMP エンジン ID とユーザ コンフィギュレーションはアクティブ ユニットから複製されます。このアクションによって、SNMP バージョン 3 クエリーの観点から、トランスペアレントなスイッチオーバーが可能になります。スイッチオーバー イベントに対応するために NMS でのコンフィギュレーション変更は必要ありません。

暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常にセキュリティ アプライアンスによって生成されます。通常は、クリア テキストの形式で入力します。

セキュリティ アプライアンスの起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

（注）　セキュリティ アプライアンス ソフトウェアをバージョン 8.0(5) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリア テキストに戻してから結果を保存する必要があります。

次に、境界インターフェイスに接続された 10.1.2.42 をホストに設定する例を示します。

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

次の例に、セキュリティ アプライアンスが SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザ、ホストの作成が含まれます。

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

次に、暗号化されたコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

次に、暗号化されていないコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server listen-port

SNMP 要求のリスニング ポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルトのポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

構文の説明

lport	着信要求が受け入れられるポート。デフォルト ポートは 161 です[1]。

1. **snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。

デフォルト

デフォルト ポートは 161 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

警告　**The UDP port *port* is in use by another feature.SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

次に、リスニング ポートを 192 に設定する例を示します。

```
hostname(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server location

SNMP のセキュリティ アプライアンスの場所を設定するには、グローバル コンフィギュレーション モードで **snmp-server location** コマンドを使用します。場所を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *text*

no snmp-server location [*text*]

構文の説明

location *text*	セキュリティ アプライアンスの場所を指定します。**location** *text* は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、SNMP のセキュリティ アプライアンスの場所を Building 42、Sector 54 として設定する例を示します。

```
hostname(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user

新しい SNMP ユーザを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。指定した SNMP ユーザを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

構文の説明

128	（任意）暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	（任意）暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	（任意）暗号化について 256 ビット AES アルゴリズムの使用を指定します。
3des	（任意）暗号化について 168 ビット 3DES アルゴリズムの使用を指定します。
aes	（任意）暗号化について AES アルゴリズムの使用を指定します。
auth	（任意）使用する認証レベルを指定します。
auth-password	（任意）エージェントがホストからパケットを受信できるようにするストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
des	（任意）暗号化について 56 ビット DES アルゴリズムの使用を指定します。
encrypted	（任意）パスワードが暗号化された形式で表示されるかどうかを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。
group-name	ユーザが属すグループの名前を指定します。
md5	（任意）HMAC-MD5-96 認証レベルを指定します。
priv	暗号化されたパケット認証を指定します。
priv-password	（任意）プライバシー ユーザ パスワードを示すストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
sha	（任意）HMAC-SHA-96 認証レベルを指定します。
username	エージェントに接続するホストのユーザ名を指定します。
v3	SNMP バージョン 3 セキュリティ モデルを使用することを指定します。**encrypted**、**priv**、または **auth** キーワードの使用を許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン

SNMP ユーザは、SNMP グループの一部である必要があります。バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザを設定した後、SNMP ホストを設定する必要があります。

（注） パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。

snmp-server user のコンフィギュレーションがコンソールに表示されるか、ファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証およびプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます。この使用法は、RFC 3414、11.2 項によって要求されています。

（注） 3DES または AES アルゴリズムを使用してユーザを設定するには、3DES または AES 機能のライセンスが必要です。

セキュリティ アプライアンスの起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、セキュリティ アプライアンスで SNMP バージョン 3 セキュリティ モデルを使用して SNMP 要求を受信する例を示します。

```
hostname(config)# snmp-server group engineering v3 auth
hostname(config)# snmp-server user engineering v3 auth sha mypassword
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
snmp-server enable	セキュリティ アプライアンスで SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを作成します。
snmp-server host	SNMP ホスト アドレスを設定します。

software-version

サーバまたはエンドポイントのソフトウェア バージョンを表示するサーバおよびユーザ エージェント ヘッダー フィールドを識別するには、パラメータ コンフィギュレーション モードで **software-version** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

software-version action {**mask** | **log**} [**log**}

no software-version action {**mask** | **log**} [**log**}

構文の説明

mask	SIP メッセージ内のソフトウェア バージョンをマスクします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップでソフトウェア バージョンを識別する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

speed

銅線（RJ-45）イーサネット インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

構文の説明

10	速度を 10BASE-T に設定します。
100	速度を 100BASE-T に設定します。
1000	速度を 1000BASE-T に設定します。銅線ギガビット イーサネットの場合のみ。
auto	速度を自動検出します。
nonegotiate	ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータをネゴシエートしません。ファイバ インターフェイスに対して使用できる設定は、このコマンドとこのコマンドの **no** 形式だけです。値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスでリンク ネゴシエーションがイネーブルになり、フロー制御パラメータとリモート障害情報が交換されます。

デフォルト

銅線インターフェイスの場合、デフォルトは **speed auto** です。

ファイバ インターフェイスの場合、デフォルトは **no speed nonegotiate** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

速度は物理インターフェイスだけで設定します。

ネットワークで自動検出がサポートされていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズの適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行す

ることでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポートで速度を **auto** 以外に設定する場合（可能な場合）、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

例

次に、速度を 1000BASE-T に設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。

split-dns

スプリット トンネルを介して解決されるドメインのリストを入力するには、グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。これにより、**split-dns none** コマンドを発行して作成されたヌル リストを含め、設定されているスプリット トンネリング ドメインのリストはすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。このようなスプリット トンネリング ドメインのリストをユーザが継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

構文の説明

value *domain-name*	スプリット トンネルを介してセキュリティ アプライアンスが解決するドメイン名を指定します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストをヌル値で設定して、スプリット DNS リストを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのスプリット DNS リストを継承しません。

デフォルト

スプリット DNS はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ドメインのリスト内の各エントリを区切るには、単一のスペースを使用します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。

no split-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成したヌル値を含め、現在の値はすべて削除されます。

AnyConnect VPN Client と SSL VPN Client はいずれもスプリット DNS をサポートしていません。

例

次に、FirstGroup という名前のグループ ポリシーに対してスプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-horizon

EIGRP スプリット ホライズンを再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **split-horizon** コマンドを使用します。EIGRP スプリット ホライズンをディセーブルにするには、このコマンドの **no** 形式を使用します。

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。

デフォルト

split-horizon コマンドはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

X.25 パケットスイッチド ネットワーク上のリンクを含むネットワークでは、**neighbor** コマンドを使用してスプリット ホライズン機能を無効にすることができます。代わりに、コンフィギュレーションで **no split-horizon eigrp** コマンドを明示的に指定することもできます。ただし、その場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、同様にスプリット ホライズンをディセーブルにする必要があります。

通常、スプリット ホライズンのデフォルトの状態は、ルートを適切にアドバタイズするために変更することがアプリケーションにおいて必要となる場合を除き、変更しないことを推奨します。シリアル インターフェイスでスプリット ホライズンがディセーブルであり、そのインターフェイスがパケットスイッチド ネットワークに接続されている場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、スプリット ホライズンをディセーブルにする必要があります。

例

次に、インターフェイス Ethernet0/0 で EIGRP スプリット ホライズンをディセーブルにする例を示します。

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# no split-horizon eigrp 100
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

split-tunnel-network-list

スプリット トンネリングのネットワーク リストを作成するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワーク リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ネットワーク リストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。これにより、**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含め、設定されているネットワーク リストはすべて削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。このようなネットワーク リストをユーザが継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

構文の説明

value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙するアクセス リストを指定します。
none	スプリット トンネリングのネットワーク リストがないことを指定します。セキュリティ アプライアンスによって、すべてのトラフィックがトンネリングされます。 スプリット トンネリング ネットワーク リストをヌル値で設定して、スプリット トンネリングを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのデフォルトのスプリット トンネリング ネットワーク リストを継承しません。

デフォルト

デフォルトでは、スプリット トンネリング ネットワーク リストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ネットワーク リストに基づいてスプリット トンネリングの判断が行われます。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成される標準 ACL です。

no split-tunnel-network-list コマンドを引数なしで使用すると、**split-tunnel-network-list none** コマンドを発行して作成したヌル値を含め、現在のネットワーク リストはすべて削除されます。

例

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

スプリット トンネリングを使用すると、リモート アクセス IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようになります。スプリット トンネリングをイネーブルにすると、宛先が IPSec トンネルの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

このコマンドでは、このスプリット トンネリング ポリシーが特定のネットワークに適用されます。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。このオプションは、Cisco VPN Client だけに適用されます。
split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、またはセキュリティ アプライアンス以外の宛先に送信しないことを指定します。リモート ユーザは、インターネット ネットワークに社内ネットワークを介してアクセスし、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

スプリット トンネリングは、デフォルト（tunnelall）ではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドの除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。

spoof-server

HTTP プロトコル インスペクションのために、サーバ ヘッダー フィールドをストリングに置き換えるには、パラメータ コンフィギュレーション モードで **spoof-server** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

spoof-server *string*

no spoof-server *string*

構文の説明

string	サーバ ヘッダー フィールドを置き換えるストリング。最大 82 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN ストリームは **spoof-server** コマンドの対象になりません。

例

次に、HTTP インスペクション ポリシー マップでサーバ ヘッダー フィールドをあるストリングに置き換える例を示します。

```
hostname(config-pmap-p)# spoof-server string
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

sq-period

NAC フレームワーク セッションで正常に完了したポスチャ検証と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **sq-period** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

sq-period *seconds*

no sq-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 30 ～ 1800 です。

デフォルト

デフォルト値は 300 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、正常に実行された各ポスチャ検証とステータス クエリー応答の後に、ステータス クエリー タイマーを起動します。このタイマーが切れると、ホスト ポスチャの変化を調べるクエリー（*ステータス クエリー*と呼ばれる）がトリガーされます。

例

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
hostname(config-nac-policy-nac-framework)# sq-period 1800
hostname(config-nac-policy-nac-framework)
```

次に、NAC フレームワーク ポリシーからステータス クエリー タイマーを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no sq-period
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
`nac-policy`	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
`nac-settings`	NAC ポリシーをグループ ポリシーに割り当てます。
`eou timeout`	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
`reval-period`	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
`debug eap`	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。

ssh

セキュリティ アプライアンスに SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。セキュリティ アプライアンスへの SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

構文の説明

interface	SSH をイネーブルにするセキュリティ アプライアンス インターフェイス。指定しない場合、SSH は外部インターフェイスを除くすべてのインターフェイスでイネーブルになります。
ip_address	セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークの IPv4 アドレス。ホストの場合は、ホスト名を入力することもできます。
ipv6_address/*prefix*	セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ssh *ip_address* コマンドでは、セキュリティ アプライアンスへの SSH 接続を開始することを認可されるホストまたはネットワークを指定します。複数の ssh コマンドをコンフィギュレーションに含めることができます。このコマンドの **no** 形式によって、特定の SSH コマンドをコンフィギュレーションから削除します。すべての SSH コマンドを削除するには、**clear configure ssh** コマンドを使用します。

セキュリティ アプライアンスへの SSH の使用を開始する前に、**crypto key generate rsa** コマンドを使用してデフォルトの RSA キーを生成する必要があります。

セキュリティ アプライアンスでは、次のセキュリティ アルゴリズムと暗号がサポートされています。

- データ暗号化のための 3DES 暗号および AES 暗号

- パケットの完全性のための HMAC-SHA アルゴリズムおよび HMAC-MD5 アルゴリズム
- ホスト認証のための RSA 公開キー アルゴリズム
- キー交換のための Diffie-Hellman Group 1 アルゴリズム

次の SSH バージョン 2 機能は、セキュリティ アプライアンスでサポートされていません。

- X11 転送
- ポート フォワーディング
- SFTP サポート
- Kerberos と AFS のチケット引き渡し
- データ圧縮

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	セキュリティ アプライアンスでセキュア コピー サーバをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

構文の説明

session_id	ID 番号で指定した SSH セッションを切断します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次に、切断される SSH セッションの例を示します。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	セキュリティ アプライアンスとのアクティブ SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh scopy enable

セキュリティ アプライアンスで Secure Copy（SCP; セキュア コピー）をイネーブルにするには、グローバル コンフィギュレーション モードで **ssh scopy enable** コマンドを使用します。SCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh scopy enable

no ssh scopy enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SCP はサーバのみの実装です。SCP のための接続を受け入れて終了できますが、開始することはできません。セキュリティ アプライアンスには、次の制約事項があります。

- SCP のこの実装にはディレクトリ サポートはないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスは制限されます。
- SCP の使用時はバナー サポートはありません。
- SCP ではワイルドカードはサポートされません。
- SSH バージョン 2 接続をサポートするには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が必要です。

ファイル転送を開始する前に、セキュリティ アプライアンスでは使用可能なフラッシュ メモリをチェックします。使用可能なスペースが十分ではない場合、セキュリティ アプライアンスは SCP 接続を終了します。フラッシュ メモリ内のファイルを上書きする場合でも、セキュリティ アプライアンスにコピーされるファイル用に十分な空きスペースが必要です。SCP プロセスでは、ファイルはまず一時ファイルにコピーされ、置き換えられるファイルに一時ファイルがコピーされます。コピーされるファイルと上書きされるファイルを保持する十分なスペースがフラッシュ内にない場合、セキュリティ アプライアンスは SCP 接続を終了します。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh scopy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、セキュリティ アプライアンスを制限します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

構文の説明

number	SSH セッションが切断される前に非アクティブである時間を分単位で指定します。有効な値は、1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は、5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ssh timeout コマンドでは、セッションが切断される前にアイドルである時間を分単位で指定します。デフォルトの時間は、5 分です。

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続のみを受け入れるように、内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。

コマンド	説明
show ssh sessions	セキュリティ アプライアンスとのアクティブ SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

セキュリティ アプライアンスが受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。デフォルト値では、セキュリティ アプライアンスへの SSH バージョン 1 接続と SSH バージョン 2 接続が許可されます。

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

構文の説明

1	SSH バージョン 1 接続のみがサポートされることを指定します。
2	SSH バージョン 2 接続のみがサポートされることを指定します。

デフォルト

デフォルトでは、SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 および 2 によって、セキュリティ アプライアンスでの使用をいずれのバージョンの SSH に限定するかを指定します。このコマンドの **no** 形式を使用すると、セキュリティ アプライアンスはデフォルトの状態、つまり、互換モード（両方のバージョンが使用可能）に戻ります。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

ssl certificate-authentication

クライアント証明書の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ssl certificate-authentication** コマンドを使用します。ssl 証明書の認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-numbe***r**

構文の説明

interface-name	選択したインターフェイスの名前。inside、management、outside などです。
port-number	TCP ポート番号。1 ～ 65535 の範囲の整数です。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、廃止された http authentication-certificate コマンドに代わるものです。

例

次に、SSL 証明書認証機能を使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl certificate-authentication interface inside port 330
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl client-version

セキュリティ アプライアンスがクライアントとして動作する場合の SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl client-version** コマンドを使用します。デフォルトの **any** に戻すには、このコマンドの **no** バージョンを使用します。このコマンドを使用すると、セキュリティ アプライアンスによって送信される SSL/TLS のバージョンを限定できます。

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

構文の説明

any	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 のみが受け入れられます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello が送信され、TLS バージョン 1 のみが受け入れられます。

デフォルト

デフォルト値は **any** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート フォワーディングは、WebVPN ユーザが次の SSL バージョンで接続している場合、動作しません。

SSLv3 でネゴシエート	Java がダウンロードされる
SSLv3/TLSv1 でネゴシエート	Java がダウンロードされる
TLSv1 でネゴシエート	Java がダウンロードされない
TLSv1 だけ	Java がダウンロードされない
SSLv3 だけ	Java がダウンロードされない

問題は、ポート フォワーディング アプリケーションを起動すると、JAVA ではクライアントの Hello パケットで SSLv3 のみがネゴシエートされることです。

例

次に、SSL クライアントとして動作する場合に TLSv1 のみを使用して通信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl client-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl encryption

SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。このコマンドを再度発行すると、前の設定は上書きされます。アルゴリズムの使用の優先順位は、アルゴリズムの順序によって決まります。環境のニーズに合わせてアルゴリズムを追加または削除できます。デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*aes128-sha1*] [*aes256-sha1*] [*possibly others*]

no ssl encryption

構文の説明

3des-sha1	Secure Hash Algorithm 1 を使用するトリプル DES 暗号化を指定します。
des-sha1	Secure Hash Algorithm 1 を使用する DES 暗号化を指定します。
rc4-md5	MD5 ハッシュ関数を使用する RC4 暗号化を指定します。
aes128-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 128 ビット暗号化を指定します。
aes256-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 256 ビット暗号化を指定します。
possibly others	今後のリリースで暗号化アルゴリズムが追加される可能性があることを示します。

デフォルト

デフォルトでは、すべてのアルゴリズムを次の順序で使用できます。

[*ssl encryption***] [***rc4-sha1***] [***aes128-sha1***] [***aes256-sha1***] [***3des-sha1***]**

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のライセンス タブには、設定した値ではなく、ライセンスでサポートされる暗号化の最大レベルが反映されます。

例

次に、3des-sha1 および des-sha1 暗号化アルゴリズムを使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl server-version

サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** バージョンを使用します。このコマンドを使用すると、セキュリティ アプライアンスによって受け入れられる SSL/TLS のバージョンを限定できます。

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

構文の説明

any	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 にネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 クライアントの hello のみが受け入れられ、SSL バージョン 3 のみが使用されます。
tlsv1	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、TLS バージョン 1 にネゴシエートされます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello のみが受け入れられ、TLS バージョン 1 のみが使用されます。

デフォルト

デフォルト値は **any** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート フォワーディングは、WebVPN ユーザが次の SSL バージョンで接続している場合、動作しません。

SSLv3 でネゴシエート	Java がダウンロードされる
SSLv3/TLSv1 でネゴシエート	Java がダウンロードされる
TLSv1 でネゴシエート	Java がダウンロードされない

TLSv1 だけ	Java がダウンロードされない
SSLv3 だけ	Java がダウンロードされない

電子メール プロキシを設定する場合、SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。

例

次に、SSL サーバとして動作する場合に TLSv1 のみを使用して通信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# ssl server-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書トラストポイントを指定するには、グローバル コンフィギュレーション モードで **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイス用のフォールバック トラストポイントが作成されます。インターフェイスを指定しない SSL トラストポイントをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。インターフェイスを指定するエントリを削除するには、このコマンドの **no ssl trust-point** {*trustpoint [interface]*} 形式を使用します。

ssl trust-point {*trustpoint [interface]*}

no ssl trust-point

構文の説明

interface	トラストポイントが適用されるインターフェイスの名前。インターフェイスの名前は **nameif** コマンドで指定します。
trustpoint	**crypto ca trustpoint** {*name*} コマンドで設定された CA トラストポイントの *name*。

デフォルト

デフォルトでは、トラストポイント アソシエーションはありません。セキュリティ アプライアンスでは、デフォルトの自己生成 RSA キー ペア証明書が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するときは、次のガイドラインに従ってください。

- *trustpoint* の値は、**crypto ca trustpoint {*name*}** コマンドで設定された CA トラストポイントの name である必要があります。
- *interface* の値は、あらかじめ設定されたインターフェイスの *nameif* 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trustpoint** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。

次に、このコマンドの **no** 形式を使用する例を示します。

このコンフィギュレーションには、次の SSL トラストポイントが含まれています。

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

次のコマンドを発行します。

no ssl trust-point

show run ssl を実行すると、次のように表示されます。

ssl trust-point tp2 outside

例

次に、内部インターフェイス用の FirstTrust という名前の ssl トラストポイントと、インターフェイスが関連付けられない DefaultTrust という名前のトラストポイントを設定する例を示します。

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

次に、このコマンドの **no** 形式を使用して、インターフェイスが関連付けられていないトラストポイントを削除する例を示します。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

次に、インターフェイスが関連付けられているトラストポイントを削除する例を示します。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコルのバージョンを指定します。

sso-server

セキュリティ アプライアンスのユーザ認証のために Single Sign-On（SSO; シングル サインオン）サーバを作成する場合、webvpn コンフィギュレーション モードで **sso-server** コマンドを使用します。このコマンドでは、SSO サーバ タイプを指定する必要があります。

SSO サーバを削除するには、このコマンドの **no** 形式を使用します。

sso-server *name* **type [***siteminder* | *saml-v1.1-post*]

no sso-server *name*

（注）　このコマンドは、SSO 認証用に必要です。

構文の説明

name	SSO サーバの名前を指定します。最小 4 文字、最大 31 文字です。
saml-v1.1-post	設定するセキュリティ アプライアンス SSO サーバが、SAML、バージョン 1.1、POST タイプの SSO サーバであることを指定します。
siteminder	設定するセキュリティ アプライアンス SSO サーバが、Computer Associates SiteMinder SSO サーバであることを指定します。
type	SSO サーバのタイプを指定します。使用できるタイプは、SiteMinder と SAML-V1.1-POST だけです。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**sso-server** コマンドを使用すると、SSO サーバを作成できます。

認証では、セキュリティ アプライアンスは SSO サーバへの WebVPN ユーザのプロキシとして動作します。セキュリティ アプライアンスは現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。現在、type オプションで使用できる引数は *siteminder* または *saml-V1.1-post* に限定されています。

例

次に、webvpn コンフィギュレーション モードで、「example1」という名前の SiteMinder-type の SSO サーバを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example1 type siteminder
hostname(config-webvpn-sso-siteminder)#
```

次に、webvpn コンフィギュレーション モードで、「example2」という名前の SAML、バージョン 1.1、POST-type の SSO サーバを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example2 type saml-v1.1-post
hostname(config-webvpn-sso-saml)#
```

関連コマンド

コマンド	説明
assertion-consumer-url	SAML-type の SSO アサーション コンシューマ サービスの URL を指定します。
issuer	SAML-type の SSO サーバのセキュリティ デバイス名を指定します。
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの運用統計情報を表示します。
test sso-server	テスト認証要求で SSO サーバをテストします。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（グループ ポリシー webvpn）

SSO サーバをグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。

デフォルト ポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	グループ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

グループに割り当てられるデフォルト ポリシーは、DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

グループ ポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

（注） SSO サーバをユーザ ポリシーに割り当てるには、同じコマンド **sso-server value** をユーザ名 webvpn コンフィギュレーション モードで入力します。

例

次に、グループ ポリシー my-sso-grp-pol を作成し、example という名前の SSO サーバに割り当てるサンプル コマンドを示します。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（ユーザ名 webvpn）	SSO サーバをユーザ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが、SiteMinder-type の SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（ユーザ名 webvpn）

SSO サーバをユーザ ポリシーに割り当てるには、ユーザ名コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

ユーザの SSO サーバ割り当てを削除するには、このコマンドの **no** 形式を使用します。

ユーザ ポリシーがグループ ポリシーから不要な SSO サーバ割り当てを継承している場合は、**sso-server none** コマンドを使用して割り当てを削除します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

構文の説明

name	ユーザ ポリシーに割り当てる SSO サーバの名前を指定します。

デフォルト

デフォルトでは、ユーザ ポリシーはグループ ポリシーの SSO サーバ割り当てを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは、現在、SiteMinder-type の SSO サーバと SAML POST-type の SSO サーバをサポートしています。

このコマンドは SSO サーバの両タイプに適用されます。

sso-server value コマンドを入力すると、SSO サーバをユーザ ポリシーに割り当てることができます。

（注）　SSO サーバをグループ ポリシーに割り当てるには、同じコマンド **sso-server value** をグループ webvpn コンフィギュレーション モードで入力します。

例

次に、my-sso-server という名前の SSO サーバを Anyuser という名前の WebVPN ユーザのユーザ ポリシーに割り当てるサンプル コマンドを示します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
```

```
hostname(config-username-webvpn)# sso-server value my-sso-server
hostname(config-username-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（config-group-webvpn）	SSO サーバをグループ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

start-url

オプションの事前ログイン クッキーの取得先 URL を入力するには、AAA サーバ ホスト コンフィギュレーション モードで **start-url** コマンドを入力します。これは HTTP フォームのコマンドを使用した SSO です。

start-url *string*

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	SSO サーバの URL。URL の最大長は 1024 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、シングル サインオン認証要求を認証 Web サーバに送信できます。認証 Web サーバは、Set-Cookie ヘッダーをログイン ページのコンテンツとともに送信することによって、事前ログイン シーケンスを実行できます。このことは、認証 Web サーバのログイン ページにブラウザで直接接続することによって検出できます。ログイン ページがロードされるときに Web サーバによってクッキーが設定され、このクッキーがその後のログイン セッションに関連する場合、**start-url** コマンドを使用してクッキーの取得先 URL を入力する必要があります。実際のログイン シーケンスは、事前ログイン クッキー シーケンスの後で、認証 Web サーバへのフォーム送信により開始されます。

（注）　**start-url** コマンドは、事前ログイン クッキー交換が存在する場合にのみ必要です。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、事前ログイン クッキーを取得するための URL https://example.com/east/Area.do?Page-Grp1 を指定する例を示します。

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

state-checking

H.323 の状態チェックを実行するには、パラメータ コンフィギュレーション モードで **state-checking** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

state-checking [h225 | ras]

no state-checking [h225 | ras]

構文の説明

h225	H.225 の状態チェックを実行します。
ras	RAS の状態チェックを実行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 コールで RAS の状態チェックを実行する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

static

実際の IP アドレスをマッピング先の IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定するには、グローバル コンフィギュレーション モードで **static** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

スタティック NAT の場合：

static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

スタティック PAT の場合：

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

構文の説明

access-list *access_list_name*	拡張アクセス リストを使用して、実アドレスおよび宛先/送信元アドレスを指定します。この機能は、ポリシー NAT と呼ばれています。
	
	拡張アクセス リストを作成するには、**access-list extended** コマンドを使用します。アクセス リストの最初のアドレスは、実アドレスです。2 番めのアドレスは、トラフィックの発生元に応じて、送信元アドレスか宛先アドレスです。たとえば、10.1.1.1 がトラフィックを 209.165.200.224 ネットワークに送信するときに、実アドレス 10.1.1.1 をマッピング先のアドレス 192.168.1.1 に変換するには、**access-list** コマンドおよび **static** コマンドは次のようになります。
	
	`hostname(config)# access-list TEST extended ip host 10.1.1.1 209.165.200.224 255.255.255.224`
	`hostname(config)# static (inside,outside) 192.168.1.1 access-list TEST`
	
	この場合、2 番めのアドレスは宛先アドレスです。ただし、ホストがマッピング先のアドレスへの接続を開始する場合にも、同じコンフィギュレーションが使用されます。たとえば、209.165.200.224 ネットワーク上のホストが 192.168.1.1 への接続を開始する場合、アクセス リストの 2 番めのアドレスは送信元アドレスです。
	
	このアクセス リストには、**permit** ACE のみを含めます。オプションで、**eq** 演算子を使用して、アクセス リストに実際のポートと宛先ポートを指定できます。ポリシー NAT では **inactive** キーワードまたは **time-range** キーワードは考慮されません。ポリシー NAT コンフィギュレーションでは、すべての ACE はアクティブであると見なされます。
	
	変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定する必要があります。

dns	（任意）このスタティックと一致する DNS 応答内の A レコード（アドレス レコード）を書き換えます。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。 **（注）** この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。
emb_lim	（任意）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 **（注）** スタティック NAT を使用して適用される初期接続の制限は、指定したインターフェイス間の接続だけでなく、実際の IP アドレスへ、または実際の IP アドレスからのすべての接続に適用されます。特定のフローだけに制限を適用するには、**set connection** コマンドを参照してください。

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。インターフェイス アドレスを使用する必要がある場合はこのキーワードを使用しますが、アドレスは、DHCP を使用してダイナミックに割り当てられます。 **（注）** インターフェイスの IP アドレスをスタティック PAT エントリに含める場合は、実際の IP アドレスを指定する代わりに **interface** キーワードを使用する必要があります。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip	実アドレスの変換先アドレスを指定します。
mapped_port	マッピング先の TCP ポートまたは UDP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
nailed	（任意）非対称でルーティングされたトラフィックの TCP セッションを許可します。このオプションを使用すると、状態を確立するための対応する発信接続がなくても、着信トラフィックはセキュリティ アプライアンスを通過できます。このコマンドは、**failover timeout** コマンドとともに使用します。**failover timeout** コマンドによって、システムが起動したかアクティブになった後に、ネイリングされたセッションが受け入れられる期間が指定されます。設定しない場合は、接続を再確立できません。 **（注）** **nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。**asr-group** コマンドを使用して非対称ルーティングのサポートを設定する方が、**static** コマンドを **nailed** オプションを指定して使用するよりもセキュアであるため、非対称ルーティングのサポートを設定する方法として推奨されます。
netmask *mask*	実アドレスおよびマッピング先のアドレスのサブネット マスクを指定します。単一ホストの場合は、255.255.255.255 を使用します。マスクを入力しない場合は、IP アドレス クラスのデフォルト マスクが使用されます。ただし、例外が 1 つあります。マスキング後のホストビットが 0 以外の場合は、ホスト マスク 255.255.255.255 が使用されます。*real_ip* の代わりに **access-list** キーワードを使用する場合、アクセス リストで使用されるサブネット マスクは *mapped_ip* にも使用されます。

norandomseq	（任意）TCP ISN のランダム化保護をディセーブルにします。それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。 保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。 TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。 • 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。 • セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実アドレスを指定します。
real_port	実際の TCP ポートまたは UDP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
tcp	スタティック PAT の場合、プロトコルを TCP として指定します。
tcp *max_conns*	ローカル ホストに許可する同時 TCP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。
udp	スタティック PAT の場合、プロトコルを UDP として指定します。
udp *udp_max_conns*	（任意）ローカル ホストに許可する同時 UDP 接続の最大数を指定します（**local-host** コマンドを参照）。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。 接続制限を設定するために推奨される方法は、ポリシー マップの中でクラスに接続制限を設定して、モジュラ ポリシー フレームワークを使用することです。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2.(1)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

スタティック NAT では、実アドレスからマッピング先のアドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは、後続の変換ごとに異なるアドレスまたはポートを使用します。スタティック NAT では連続する各接続においてマッピング先のアドレスは同じであり、固定の変換ルールが存在するため、スタティック NAT では、宛先ネットワーク上のホストは変換されたホストへのトラフィックを開始できます（それを許可するアクセス リストがある場合）。

（注） スタティック ポリシー NAT の場合、変換の取り消しにおいて、**static** コマンド内の ACL は使用されません。パケット内の宛先アドレスがスタティック ルールのマッピング先のアドレスと一致する場合は、アドレスを未変換の状態に戻すのに、スタティック ルールが使用されます。

ダイナミック NAT と、スタティック NAT のアドレス範囲との主な違いは、スタティック NAT では、変換されたホストへの接続をリモート ホストが開始できるが（それを許可するアクセス リストがある場合）、ダイナミック NAT ではできないことです。また、スタティック NAT では、実アドレスと同じ数のマッピング先のアドレスが必要です。

スタティック ポリシー NAT では一致するポートの使用がサポートされていますが、NAT ではサポートされていません。

スタティック PAT はスタティック NAT と同じですが、実アドレスとマッピング先のアドレスに対してプロトコル（TCP または UDP）およびポートを指定できる点が異なります。

この機能を使用すると、複数の異なる static ステートメントで同じマッピング先のアドレスを指定できます。ただし、ステートメントごとにポートが異なる必要があります（複数のスタティック NAT ステートメントに対して同じマッピング先のアドレスを使用することはできません）。

スタティック PAT を使用しない限り、同じ 2 つのインターフェイス間の、複数の **static** コマンドで、同じ実アドレスまたはマッピング先のアドレスを使用することはできません。同じマッピングされているインターフェイスに対して、**global** コマンドでも定義されているマッピング先のアドレスを **static** コマンドで使用しないでください。

セカンダリ チャネルのアプリケーション インスペクションを必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定する必要があります。

static コマンド ステートメントを変更または削除した後は、**clear xlate** コマンドを使用して変換をクリアします。

また、**set connection** コマンドを使用して、最大接続数、最大初期接続数、および TCP シーケンスのランダム化を設定できます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

接続属性（**dns**、**norandomseq**、**nailed**、**tcp**、および **udp**）には、ホスト単位の制限があります。ポリシー NAT（アクセス リストを使用）や 3 つ以上のインターフェイスがある NAT などの場合、複数の **nat** コマンドと **static** コマンドから接続属性の値を生成できます。そのような場合、最初のパケットと一致するルールの値が、優先される値です。たとえば、次のコンフィギュレーションでは、TCP 接続制限 100 および 200 を適用できます。

```
static (inside,dmz) 192.168.1.1 192.168.1.100 tcp 100
static (inside,outside) 192.168.1.1 192.168.1.100 tcp 200
```

ホスト 192.168.1.1 からの最初のパケットが dmz インターフェイス向けである場合、その後のすべての TCP セッションで TCP 接続制限は 100 です。

例

スタティック NAT の例

たとえば、次のポリシー スタティック NAT の例は、宛先アドレスに応じて 2 つのマッピング先のアドレスに変換される単一の実アドレスを示しています。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドでは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングします。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255
```

次のコマンドでは、外部アドレス（209.165.201.15）を内部アドレス（10.1.1.6）にマッピングします。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
```

次のコマンドでは、サブネット全体をスタティックにマッピングします。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

次に、限定された数のユーザが Intel Internet Phone、CU-SeeMe、CU-SeeMe Pro、MeetingPoint、または Microsoft NetMeeting を使用して H.323 経由でコール インできるようにする例を示します。**static** コマンドでは、アドレス 209.165.201.0 ～ 209.165.201.30 をローカル アドレス 10.1.1.0 ～ 10.1.1.30 にマッピングします（209.165.201.1 が 10.1.1.1 にマッピング、209.165.201.10 が 10.1.1.10 にマッピングなど）。

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask 255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq h323
hostname(config)# access-group acl_out in interface outside
```

次の例は、Mail Guard をディセーブルにするために使用するコマンドを示しています。

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

この例では、**static** コマンドによって、外部ホストが dmz1 インターフェイス上にある 10.1.1.1 メール サーバ ホストにアクセスできるようにするグローバル アドレスを設定できます。DNS の MX レコードを 209.165.201.1 アドレスを指定するように設定し、メールがこのアドレスに送信されるようにする必要があります。**access-list** コマンドにより、外部ユーザは SMTP ポート（25）を通じてグローバル アドレスにアクセスできます。**no fixup protocol** コマンドにより、Mail Guard はディセーブルになります。

スタティック PAT の例

たとえば、10.1.3.0 ネットワーク上のホストからセキュリティ アプライアンス外のインターフェイス（10.1.2.14）に向かって開始される Telnet トラフィックの場合、次のコマンドを入力することによって、10.1.1.15 にある内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

10.1.3.0 ネットワーク上のホストからセキュリティ アプライアンス外のインターフェイス（10.1.2.14）に向かって開始される HTTP トラフィックの場合、次のように入力することによって、10.1.1.15 にある内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

Telnet トラフィックをセキュリティ アプライアンス外部インターフェイス（10.1.2.14）から内部ホスト 10.1.1.15 にリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
```

ただし、上記の実際の Telnet サーバが接続を開始できるようにするには、変換を追加する必要があります。たとえば、その他のすべてのタイプのトラフィックを変換するには、次のコマンドを入力します。元の **static** コマンドは、Telnet からサーバへの変換を行います。一方、**nat** コマンドと **global** コマンドは、サーバからの発信接続のための PAT を指定します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

すべての内部トラフィックについて個別の変換も保持し、内部ホストが Telnet サーバとは異なるマッピング先のアドレスを使用する場合でも、Telnet サーバから開始されるトラフィックが、サーバへの Telnet トラフィックを許可する **static** ステートメントと同じマッピング先のアドレスを使用するように設定できます。Telnet サーバ専用の、より排他的な **nat** ステートメントを作成する必要があります。**nat** ステートメントは最も一致しているものが読み取られるため、より排他的な **nat** ステートメントは一般的なステートメントよりも前に一致します。次に、Telnet の **static** ステートメント、Telnet サーバから開始されるトラフィック用の、より排他的な **nat** ステートメント、および異なるマッピング先のアドレスを使用する他の内部ホスト用のステートメントの例を示します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

well-known ポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションから **static** コマンドを削除します。
clear xlate	すべての変換をクリアします。
nat	ダイナミック NAT を設定します。
show running-config static	コンフィギュレーション内のすべての **static** コマンドを表示します。
timeout conn	接続のタイムアウトを設定します。

strict-header-validation

RFC 3261 に従って、SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにするには、パラメータ コンフィギュレーション モードで **strict-header-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

no strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで SIP ヘッダー フィールドの厳密な検証をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

strict-http

HTTP に準拠していないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには **http-map** コマンドを使用してアクセスできます。この機能をデフォルトの動作にリセットするには、このコマンドの **no** 形式を使用します。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信して接続を閉じます。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

厳密な HTTP インスペクションをディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠していないトラフィックの転送がセキュリティ アプライアンスで許可されます。このコマンドによって、デフォルトの動作（HTTP に準拠していないトラフィックの転送を拒否する）が上書きされます。

例

次に、HTTP に準拠していないトラフィックの転送を許可する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

strip-group

このコマンドは、user@realm の形式で受信されるユーザ名にのみ適用されます。レルムは、「@」デリミタを使用してユーザ名に追加される管理ドメインです（juser@abc など）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性モードで **strip-group** コマンドを使用します。セキュリティ アプライアンスでは、VPN クライアントによって提示されるユーザ名からグループ名を取得して、IPSec 接続のトンネル グループを選択します。グループ除去処理をイネーブルにすると、セキュリティ アプライアンスでは、ユーザ名のユーザ部分のみを認可 / 認証のために送信します。それ以外の場合（ディセーブルの場合）、セキュリティ アプライアンスではレルムを含むユーザ名全体を送信します。

グループ除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-group

no strip-group

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル タイプだけに適用できます。

（注） MSCHAPv2 の制限により、MSCHAPv2 を PPP 認証に使用すると、トンネル グループのスイッチングを実行できません。MSCHAPv2 中のハッシュ計算はユーザ名の文字列にバインドされます（ユーザ + 区切り + グループなど）。

例

次に、IPSec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してグループ除去をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理によって、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムが削除されます。レルムは、@ デリミタを使用してユーザ名に追加される管理ドメインです（username@realm など）。このコマンドをイネーブルにすると、セキュリティ アプライアンスでは、ユーザ名のユーザ部分のみを認可/認証のために送信します。それ以外の場合、セキュリティ アプライアンスではユーザ名全体を送信します。

レルム除去処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

strip-realm

no strip-realm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル タイプだけに適用できます。

例

次に、IPSec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してレルム除去をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-realm
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループまたは指定されたトンネル グループをクリアします。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

storage-key

セッション間に保管されるデータを保護するストレージ キーを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-key** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- key { **none** | **value** <*string*>}

no storage-key

構文の説明

string	ストレージ キーの値として使用するストリングを指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ストレージ キーの値にはスペース以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。

例

次に、ストレージ キーを値 abc123 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-key value abc123
```

関連コマンド

コマンド	説明
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

storage-objects

セッション間に保管されるデータについて使用するストレージ オブジェクトを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **storage-objects** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

storage- objects { **none** | **value** <*string*>}

no storage-objects

構文の説明

string	ストレージ オブジェクトの名前を指定します。この文字列は最大 64 文字まで使用できます。

デフォルト

デフォルトは **none** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ストレージ オブジェクト名にはスペースおよびカンマ以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。ストリング内でストレージ オブジェクトの名前を区切るには、カンマをスペースなしで使用します。

例

次に、ストレージ オブジェクト名を cookies および xyz456 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-object value cookies,xyz456
```

関連コマンド

コマンド	説明
storage-key	セッション間に保管されるデータに対して使用するストレージ キーを設定します。
user-storage	セッション間にユーザ データを保管するための場所を設定します。

subject-name（クリプト CA 証明書マップ）

IPSec ピア証明書のサブジェクト DN にルール エントリが適用されることを指定するには、クリプト CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

構文の説明

attr *tag*	証明書 DN の指定された属性値のみがルール エントリ ストリングと比較されることを指定します。タグ値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代識別子 I = イニシャル GN = 姓名の名 N = 名前 SN = 姓名の姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = タイトル O = 組織名 L = 地名 SP = 州 / 都道府県 C = 国 OU = 組織ユニット CN = 一般名
co	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングである必要があることを指定します。
eq	DN ストリングまたは指定された属性がルール ストリング全体と一致する必要があることを指定します。
nc	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングでないことが必要であることを指定します。
ne	DN ストリングまたは指定された属性がルール ストリング全体と一致しないことが必要であることを指定します。
string	照合される値を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA 証明書マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、証明書マップ 1 に対して CA 証明書マップ モードを開始し、証明書サブジェクト名の組織属性が Central と等しくなる必要があることを指定するルール エントリを作成する例を示します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
issuer-name	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

subject-name（クリプト CA トラスト ポイント）

指定したサブジェクト DN を登録時に証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。これは、証明書を使用する人またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

構文の説明

X.500_name	X.500 認定者名を定義します。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。たとえば、**cn=crl,ou=certs,o="cisco systems, inc.",c=US** です。最大長は 500 文字です。

デフォルト

デフォルト設定では、サブジェクト名は含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始し、URL https//:frog.phoobin.com での自動登録を設定し、サブジェクト DN OU certs をトラストポイント central の登録要求に含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=certs
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment url	CA に対する登録用の URL を指定します。

subject-name-default

ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に追加される一般的なサブジェクト名 DN を指定するには、CA サーバ コンフィギュレーション モードで **subject-name-default** コマンドを使用します。サブジェクト名 DN をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

subject-name-default *dn*

no subject-name-default

構文の説明

dn	ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に含める一般的なサブジェクト名 DN を指定します。サポートされている DN 属性は、cn（一般名）、ou（組織ユニット）、ol（組織の地名）、st（州）、ea（電子メール アドレス）、c（会社）、t（タイトル）、および sn（姓名の姓）です。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。*dn* に使用できる文字数は最大 500 文字です。

デフォルト

このコマンドは、デフォルトのコンフィギュレーションの一部ではありません。このコマンドでは、証明書のデフォルトの DN を指定します。ユーザ入力に DN がある場合、このコマンドはセキュリティ アプライアンスによって無視されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

subject-name-default コマンドでは、発行される証明書のサブジェクト名を構成するユーザ名で使用される、共通の一般的な認定者名を指定します。この目的には、*dn* 値は cn=username で十分です。このコマンドによって、ユーザごとに個別にサブジェクト名 DN を定義する必要がなくなります。

セキュリティ アプライアンスでは、このコマンドは、ユーザ入力で DN が指定されない場合に、証明書を発行するときにのみ使用されます。**crypto ca server user-db add** dn *dn* コマンドを使用してユーザが追加される場合、DN フィールドは任意です。

例

次に、DN を指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書、発行済みの証明書、または CRL のライフタイムを指定します。

summary-address（OSPF）

OSPF の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

構文の説明

addr	アドレス範囲に対して指定されるサマリー アドレスの値。
mask	集約ルートに対して使用される IP サブネット マスク。
not-advertise	（任意）指定されたプレフィックス/マスク ペアと一致するルートを抑制します。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックス/マスク ペアと一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

他のルーティング プロトコルから学習したルートをサマライズできます。このコマンドを OSPF に対して使用すると、OSPF Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）により、このアドレスの対象となる再配布されるすべてのルートの集約として、1 つの外部ルートがアドバタイズされます。このコマンドでは、OSPF に再配布されている、他のルーティング プロトコルからのルートのみが集約されます。OSPF エリア間のルート集約には **area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を、任意のキーワードまたは引数を指定しないで使用します。コンフィギュレーションの summary コマンドからオプションを削除するには、このコマンドの **no** 形式を使用して、削除するオプションを指定します。詳細については、「例」を参照してください。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
area range	エリア境界でルートを統合および集約します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

summary-address（EIGRP）

特定のインターフェイスの EIGRP のサマリーを設定するには、インターフェイス コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスを削除するには、このコマンドの **no** 形式を使用します。

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

構文の説明

as-number	自律システム番号。これは、EIGRP ルーティング プロセスの自律システム番号と同じである必要があります。
addr	サマリー IP アドレス。
mask	IP アドレスに適用されるサブネット マスク。
admin-distance	（任意）集約ルートのアドミニストレーティブ ディスタンス。有効な値は、0 ～ 255 です。指定されていない場合、デフォルト値は 5 です。

デフォルト

デフォルトの設定は次のとおりです。

- EIGRP は、単一のホスト ルートの場合でも、ルートをネットワーク レベルに自動的に集約します。
- EIGRP 集約ルートのアドミニストレーティブ ディスタンスは 5 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。自動ルート集約をディセーブルにするには、**no auto-summary** コマンドを使用します。**summary-address** コマンドを使用すると、サブネット ルート集約をインターフェイス単位で手動で定義できます。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
auto-summary	EIGRP ルーティング プロセスのサマリー アドレスを自動的に作成します。

sunrpc-server

SunRPC サービス テーブルのエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **]** **timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

構文の説明

ifc_name	サーバ インターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [- *port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（任意）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC トランスポート プロトコルを指定します。
protocol udp	SunRPC トランスポート プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SunRPC サービス テーブルは、timeout で指定された時間、確立された SunRPC セッションに基づいて、SunRPC トラフィックがセキュリティ アプライアンスを通過するのを許可するために使用します。

例

次に、SunRPC サービス テーブルを作成する例を示します。

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスからの Sun リモート プロセッサ コール サービスをクリアします。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に対して認証されている場合に、このトラストポイントに基づいてリモート証明書を検証するには、クリプト CA トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定では、ユーザ証明書の検証がサポートされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central でユーザ検証を受け入れることができるようにする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

svc ask

セキュリティ アプライアンスがリモート SSL VPN クライアント ユーザに対してクライアントのダウンロードを促せるようにするには、グループ ポリシー WebVPN またはユーザ名 webvpn コンフィギュレーション モードから **svc ask** コマンドを使用します。

コンフィギュレーションからコマンドを削除するには、このコマンドの no 形式を使用します。

svc ask {**none** | **enable** [**default** {**webvpn** | **svc**} **timeout** *value*]}

no svc ask none [**default** {**webvpn** | **svc**}]

構文の説明

none	デフォルト アクションをただちに実行します。
enable	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動してユーザ応答を無期限に待機します。
default svc timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション（クライアントのダウンロード）を実行します。
default webvpn timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション（WebVPN ポータル ページの表示）を実行します。

デフォルト

このコマンドのデフォルトは、**svc ask none default webvpn** です。セキュリティ アプライアンスによって、クライアントレス接続のポータル ページがただちに表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

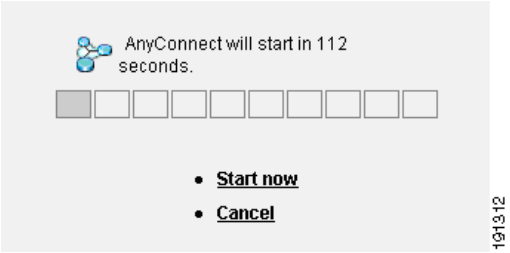
コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

図 31-1 に、**default svc timeout** *value* または **default webvpn timeout** *value* が設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 31-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



例

次に、セキュリティ アプライアンスを設定して、リモート ユーザにクライアントのダウンロードを要求するか、ポータル ページに移動して、ユーザの応答を 10 秒待機してからクライアントをダウンロードするように設定する例を示します。

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc compression

特定のグループまたはユーザについて、SSL VPN 接続での http データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc compression** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

構文の説明

deflate	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

デフォルト

デフォルトでは、圧縮は *none*（ディセーブル）に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

SSL VPN 接続の場合、webvpn コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **svc compression** コマンドは上書きされます。

例

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

関連コマンド

コマンド	説明
compression	すべての SSL、WebVPN、および IPSec VPN 接続で、圧縮をイネーブルにします。
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。

svc dpd-interval

Dead Peer Detection（DPD; デッド ピア検出）をセキュリティ アプライアンスでイネーブルにし、リモート クライアントとセキュリティ アプライアンスのいずれかで SSL VPN 接続を介した DPD を実行する頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで **svc dpd-interval** コマンドを使用します。

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

構文の説明

gateway *seconds*	セキュリティ アプライアンスで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
gateway none	セキュリティ アプライアンスで実行される DPD をディセーブルにします。
client *seconds*	クライアントで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
client none	クライアントで実行される DPD をディセーブルにします。

デフォルト

デフォルトでは、DPD はイネーブルであり、セキュリティ アプライアンス（ゲートウェイ）とクライアントの両方で 30 秒に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(3)	デフォルト設定が、ディセーブルから、セキュリティ アプライアンス（ゲートウェイ）とクライアントの両方で 30 秒に変更されました。

例

次の例では、ユーザは、既存のグループ ポリシー *sales* について、セキュリティ アプライアンス（ゲートウェイ）で実行される DPD の頻度を 3000 秒に設定し、クライアントで実行される DPD の頻度を 1000 秒に設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc keepalive	リモート コンピュータ上のクライアントからセキュリティ アプライアンスにキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
svc rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。

svc dtls enable

Cisco AnyConnect VPN Client との SSL VPN 接続を確立している特定のグループまたはユーザのインターフェイスで Datagram Transport Layer Security（DTLS）接続をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで **dtls enable** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

dtls enable *interface*

no dtls enable *interface*

構文の説明

interface	インターフェイスの名前。

デフォルト

デフォルトではイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

DTLS をイネーブルにすると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立する AnyConnect クライアント ユーザは SSL トンネル経由でだけ接続できます。

このコマンドでは、特定のグループまたはユーザについて DTLS をイネーブルにします。すべての AnyConnect クライアント ユーザについて DTLS をイネーブルにするには、webvpn コンフィギュレーション モードで **dtls enable** コマンドを使用します。

例

次に、グループ ポリシー *sales* のグループ ポリシー webvpn コンフィギュレーション モードを開始し、DTLS をイネーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dtls enable
```

関連コマンド

コマンド	説明
dtls port	DTLS の UDP ポートを指定します。
svc dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	セキュリティ アプライアンスがリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

svc enable

セキュリティ アプライアンスがリモート コンピュータに SSL VPN クライアントをダウンロードできるようにするには、webvpn コンフィギュレーション モードで **svc enable** コマンドを使用します。

コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

svc enable

no svc enable

デフォルト

このコマンドのデフォルトはディセーブルです。セキュリティ アプライアンスによってクライアントはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

no svc enable コマンドを入力しても、アクティブなセッションは終了しません。

例

次の例では、ユーザはセキュリティ アプライアンスによってクライアントをダウンロードできるようにします。

```
(config)# webvpn
(config-webvpn)# svc enable
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

svc profiles	セキュリティ アプライアンスによって Cisco AnyConnect VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開する SSL VPN クライアント パッケージ ファイルを指定します。

svc image

リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN クライアント パッケージ ファイルを指定するには、webvpn コンフィギュレーション モードで **svc image** コマンドを使用します。

コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

svc image *filename order* [**regex** *expression*]

no svc image *filename order* [**regex** *expression*]

構文の説明

filename	パッケージ ファイルのファイル名を最大 255 文字で指定します。
order	クライアント パッケージ ファイルが複数である場合は、*order* によってパッケージ ファイルの順序（1 ～ 65535）を指定します。セキュリティ アプライアンスでは、オペレーティング システムと一致するまで、指定した順序に従って、各クライアントの一部をリモート PC にダウンロードします。
regex *expression*	ブラウザから渡される User-Agent ストリングと照合するためにセキュリティ アプライアンスによって使用されるストリングを指定します。

デフォルト

デフォルトの順序は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。
8.0(1)	**regex** *expression* 引数が追加されました。

使用上のガイドライン

パッケージ ファイルの番号付けにより、セキュリティ アプライアンスが、オペレーティング システムと一致するまで、パッケージ ファイルの一部をリモート PC にダウンロードする順序が確立されます。最も番号の小さいパッケージ ファイルが最初にダウンロードされます。したがって、リモート PC で最も一般的に使用されるオペレーティング システムと一致するパッケージ ファイルに、最も小さい番号を割り当てる必要があります。

デフォルトの順序は 1 です。*order* 引数を指定しない場合は、**svc image** コマンドを入力するたびに、以前に番号 1 と見なされたイメージに上書きします。

クライアント パッケージ ファイルごとに任意の順序で **svc image** コマンドを入力できます。たとえば、2 番め（*order* 2）にダウンロードされるパッケージ ファイルを指定してから、最初（*order* 1）にダウンロードされるパッケージ ファイルを指定する **svc image** コマンドを入力できます。

モバイル ユーザの場合、**regex** keyword を使用して、モバイル デバイスの接続時間を短縮できます。ブラウザがセキュリティ アプライアンスに接続するとき、User-Agent ストリングが HTTP ヘッダーに含められます。セキュリティ アプライアンスによってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

セキュリティ アプライアンスでは、SSL VPN クライアントと Cisco Secure Desktop（CSD）の両方のパッケージ ファイルがキャッシュ メモリに展開されます。セキュリティ アプライアンスでパッケージ ファイルを正常に展開するには、パッケージ ファイルのイメージとファイルを保管するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことをセキュリティ アプライアンスが検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドを使用してパッケージ ファイルをインストールしようとした後でレポートされるエラー メッセージの例を示します。

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0.0070-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

パッケージ ファイルをインストールしようとしたときにこのエラーが発生した場合は、グローバル コンフィギュレーション モードで **dir cache:/** コマンドを使用して、残っているキャッシュ メモリの量と以前にインストールしたパッケージのサイズを調べます。それに応じて、webvpn コンフィギュレーション モードで **cache-fs limit** コマンドを使用して、キャッシュ サイズの制限を調整します。

例

次の例では、**show webvpn svc** コマンドの出力により、windows.pkg ファイルの順序番号が 1 であり、windows2.pkg ファイルの順序番号が 15 であることが示されます。リモート コンピュータによって接続が確立されるときに、windows.pkg ファイルが最初にダウンロードされます。このファイルがオペレーティング システムと一致しない場合、windows2.pkg ファイルがダウンロードされます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 15
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

次に、ユーザは **svc image** コマンドを使用してパッケージ ファイルの順序を変更します。windows2.pkg ファイルをリモート PC にダウンロードされる最初のファイルとし、windows.pkg ファイルを 2 番めにダウンロードされるようにします。

```
hostname(config-webvpn)# svc image windows2.pkg 10
hostname(config-webvpn)# svc image windows.pkg 20
```

show webvpn svc コマンドを再入力すると、ファイルの新しい順序が表示されます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 10
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 20
  CISCO STC win2k+ 1.0.0
  1,0,0,164
```

```
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

次に、CSD イメージ（sdesktop 内に存在）と SSL VPN クライアント イメージ（stc 内に存在）によって約 5.44 MB のキャッシュ メモリが使用されている例を示します。十分なキャッシュ メモリを作成するために、ユーザがキャッシュ サイズの制限を 6 MB に設定しています。

```
hostname(config-webvpn)# dir cache:

Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)

hostname(config-webvpn)# cache-fs limit 6
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
cache-fs limit	キャッシュ メモリのサイズを制限します。
dir cache:	キャッシュ メモリの内容を表示します。
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc enable	セキュリティ アプライアンスによってクライアントをリモート コンピュータにダウンロードできるようにします。

svc keepalive

SSL VPN 接続でリモート クライアントからセキュリティ アプライアンスに送信されるキープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc keepalive** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc keepalive {**none** | *seconds*}

no svc keepalive {**none** | *seconds*}

構文の説明

none	キープアライブ メッセージをディセーブルにします。
seconds	キープアライブ メッセージをイネーブルにし、メッセージの頻度（15 ～ 600 秒）を指定します。

デフォルト

デフォルトは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(3)	デフォルト設定がディセーブルから 20 秒に変更されました。

使用上のガイドライン

従来の Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN Client の両方で、セキュリティ アプライアンスへの SSL VPN 接続を確立するときにキープアライブ メッセージを送信できます。

接続をアイドル状態で維持できる時間がデバイスによって制限されている場合も、プロキシ、ファイアウォール、または NAT デバイスを経由した SSL VPN 接続が確実に開いたままで保たれるように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

（注）　キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

例

次の例では、ユーザは、*sales* という名前の既存のグループ ポリシーについて、セキュリティ アプライアンスを設定し、クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにします。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
svc dpd-interval	セキュリティ アプライアンスで Dead Peer Detection（DPD; デッド ピア検出）をイネーブルにし、クライアントまたはセキュリティ アプライアンスによって DPD が実行される頻度を設定します。
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
svc rekey	セッションでクライアントがキーの再生成を実行できるようにします。

svc keep-installer

リモート PC への SSL VPN クライアントの永続インストールをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc keep-installer** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

構文の説明

installed	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続に備えてリモート PC にインストールされたままとなります。
none	アクティブな接続の終了後にクライアントがリモート コンピュータからアンインストールされることを指定します。

デフォルト

デフォルトでは、クライアントの永続インストールがイネーブルです。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、ユーザはグループ ポリシー webvpn コンフィギュレーション モードを開始し、セッションの終了時にクライアントを削除するようにグループ ポリシーを設定します。

```
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)# svc keep-installer none
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスにインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
svc	特定のグループまたはユーザに対してクライアントをイネーブルまたは必須にします。
svc enable	セキュリティ アプライアンスがクライアント ファイルをリモート PC にダウンロードできるようにします。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc modules

オプション機能のために AnyConnect SSL VPN Client で必要となるオプション モジュールの名前を指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc modules** コマンドを使用します。

コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

svc modules {**none** | **value** *string*}

no svc modules {**none** | **value** *string*}

構文の説明

string	オプション モジュールの名前（最大 256 文字）。複数のストリングを指定する場合は、カンマで区切ります。

デフォルト

デフォルトは none です。セキュリティ アプライアンスによってオプション モジュールはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ダウンロード時間を最小にするために、クライアントでは、サポートする各機能に必要なモジュールのダウンロード（セキュリティ アプライアンスから）のみを要求します。**svc modules** コマンドにより、セキュリティ アプライアンスでこれらのモジュールをダウンロードできます。**none** を選択すると、セキュリティ アプライアンスによって基本的なファイルがダウンロードされ、オプションのモジュールはダウンロードされません。

vpngina ストリングを使用して、Start Before Logon（SBL）機能をイネーブルにします。このストリングにより、セキュリティ アプライアンスでは AnyConnect クライアント VPN 接続用の Graphical Identification and Authentication（GINA）をダウンロードできます。

すべてのクライアント機能に入力する値の一覧については、Cisco AnyConnect VPN Client のリリースノートを参照してください。

例

次の例では、ユーザはグループ ポリシー *telecommuters* でグループ ポリシー属性モードを開始し、そのグループ ポリシーで webvpn コンフィギュレーション モードを開始し、ストリング *vpngina* を指定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

関連コマンド

コマンド	説明
show webvpn svc	セキュリティ アプライアンスのキャッシュ メモリにロードされていてダウンロード可能な SSL VPN クライアントについての情報を表示します。
svc enable	特定のグループまたはユーザに対して、SSL VPN クライアントをイネーブルにします。
svc image	リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN クライアント パッケージ ファイルを指定します。

svc mtu

Cisco AnyConnect VPN Client によって確立された SSL VPN 接続の MTU サイズを調整するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**svc mtu** コマンドを使用します。

コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

svc mtu *size*

no svc mtu *size*

構文の説明

size	MTU サイズ（バイト単位）。256 ～ 1406 バイトです。

デフォルト

デフォルトのサイズは 1406 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、AnyConnect クライアントのみに影響します。Cisco SSL VPN Client（SVC）は、異なる MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no svc mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

このコマンドは、SSL のみで確立された AnyConnect クライアント接続と、DTLS を使用する SSL で確立された AnyConnect クライアント接続に影響します。

例

次に、グループ ポリシー *telecommuters* について、MTU サイズを 500 バイトに設定する例を示します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc mtu 500
```

関連コマンド

コマンド	説明
svc keep-installer	クライアントの自動アンインストール機能をディセーブルにします。初期ダウンロード後、接続が終了した後もクライアントはリモート PC 上に残ります。
svc dtls	SSL VPN 接続を確立するクライアントに対して DTLS をイネーブルにします。
show run webvpn	**svc** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。

svc profiles（グループ ポリシーまたはユーザ名属性）

Cisco AnyConnect VPN Client ユーザにダウンロードされるプロファイル パッケージを指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで、**svc profile** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

svc profiles {**value** *profile* | **none**}

no svc profiles {**value** *profile* | **none**}

構文の説明

profile	プロファイル名。

デフォルト

デフォルトは none です。セキュリティ アプライアンスによってプロファイルはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで入力すると、セキュリティ アプライアンスによってグループ ポリシーまたはユーザ名に基づいてプロファイルをユーザにダウンロードできます。プロファイルをすべてのユーザにダウンロードするには、このコマンドを webvpn コンフィギュレーション モードで使用します。

プロファイルは設定パラメータのグループであり、クライアントによって、ホスト コンピュータの名前やアドレスを含めて、クライアント ユーザ インターフェイスに表示される接続エントリの設定に使用されます。AnyConnect ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。

クライアント インストールには、編集可能なプロファイル テンプレート（AnyConnectProfile.tmpl）が含まれており、別のプロファイル ファイルを作成するための基本として使用できます。プロファイルの編集について詳しくは、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次の例では、ユーザは使用可能なプロファイルを表示する **svc profiles value** コマンドを照会します。

```
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

ユーザはその後、プロファイル *sales* を使用するようグループ ポリシーを設定しています。

```
asa1(config-group-webvpn)# svc profiles sales
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
svc image	リモート PC へのダウンロードのためにセキュリティ アプライアンスがキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

svc profiles（webvpn）

セキュリティ アプライアンスによってキャッシュ メモリにロードされて、Cisco AnyConnect VPN Client ユーザのグループ ポリシーおよびユーザ属性で使用可能となるプロファイル パッケージとして、ファイルを指定するには、webvpn コンフィギュレーション モードで **svc profile** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除し、セキュリティ アプライアンスによってパッケージ ファイルがキャッシュ メモリからアンロードされるようにするには、このコマンドの **no** 形式を使用します。

svc profiles {*profile path*}

no svc profiles {*profile path*}

構文の説明

path	セキュリティ アプライアンスのフラッシュ メモリ内のプロファイル ファイルのパスおよびファイル名。
profile	キャッシュ内に作成するプロファイルの名前。

デフォルト

デフォルトは none です。プロファイル パッケージはセキュリティ アプライアンスによってキャッシュ メモリにロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

プロファイルは設定パラメータのグループであり、AnyConnect クライアントによって、ホスト コンピュータの名前やアドレスを含めて、ユーザ インターフェイスに表示される接続エントリの設定に使用されます。クライアント ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。

また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。クライアント インストールには、編集可能なプロファイル テンプレート（AnyConnectProfile.tmpl）が含まれており、別のプロファイル ファイルを作成するための基本として使用できます。プロファイルの編集について詳しくは、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

新しいプロファイルを作成してフラッシュ メモリにアップロードした後、webvpn コンフィギュレーション モードで **svc profiles** コマンドを使用して、セキュリティ アプライアンスに対して XML ファイルをプロファイルとして指定します。このコマンドによって、ファイルはセキュリティ アプライアン

ス上のキャッシュ メモリにロードされます。次に、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **svc profiles** コマンドを使用して、グループまたはユーザのプロファイルを指定できます。

例

次の例では、ユーザはまずクライアントのインストールに付属する AnyConnectProfile.tmpl ファイルから 2 つの新規プロファイル ファイル（sales_hosts.xml と engineering_hosts.xml）を作成し、セキュリティ アプライアンスのフラッシュ メモリにアップロードしています。

さらに、ユーザはそれらのファイルを AnyConnect のプロファイルとしてセキュリティ アプライアンスに指定し、*sales* と *engineering* という名前を指定しています。

```
asa1(config-webvpn)# svc profiles sales disk0:sales_hosts.xml
asa1(config-webvpn)# svc profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles コマンドを入力すると、キャッシュ メモリにロードされたプロファイルが表示されます。

```
asa1(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
asa1(config-webvpn)#
```

これで、これらをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードでの **svc profiles** コマンドで使用できます。

```
asa1(config)# group-policy sales attributes
asa1(config-group-policy)# webvpn
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロード用にセキュリティ アプライアンスによってキャッシュ メモリに展開されている SSL VPN パッケージ ファイルを指定します。

svc rekey

SSL VPN 接続でリモート クライアントがキーの再生成を実行できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **svc rekey** コマンドを使用します。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

構文の説明

method ssl	キーの再生成中に SSL の再ネゴシエーションが行われることを指定します。
method new-tunnel	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
time *minutes*	セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。4 ～ 10080（1 週間）の範囲です。
method none	キーの再生成をディセーブルにします。

デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

従来の Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN クライアントは、両方ともセキュリティ アプライアンスへの SSL VPN 接続上でキーの再作成を実行できます。

キーの再生成方法として SSL を設定することを推奨します。

例

次の例では、ユーザは、グループ ポリシー *sales* に属するリモート クライアントがキーの再生成時に SSL と再ネゴシエートし、セッションの開始後 30 分でキーの再生成が発生することを指定します。

```
hostname(config)# group-policy sales attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc rekey method ssl
hostname(config-group-webvpn)# svc rekey time 30
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して AnyConnect クライアントをイネーブルまたは必須にします。
svc dpd-interval	Dead Peer Detection（DPD; デッド ピア検出）をセキュリティ アプライアンスでイネーブルにし、AnyConnect クライアントまたはセキュリティ アプライアンスのいずれかで DPD を実行する頻度を設定します。
svc keepalive	リモート コンピュータ上の AnyConnect クライアントからセキュリティ アプライアンスにキープアライブ メッセージが送信される頻度を指定します。
svc keep-installer	リモート コンピュータへの AnyConnect クライアントの永続インストールをイネーブルにします。

switchport access vlan

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用して、スイッチ ポートを VLAN に割り当てます。

switchport access vlan *number*

no switchport access vlan *number*

構文の説明

vlan *number*	このスイッチ ポートを割り当てる VLAN ID を指定します。VLAN ID の範囲は 1 ～ 4090 です。

デフォルト

デフォルトでは、すべてのスイッチ ポートが VLAN 1 に割り当てられています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

トランスペアレント ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで 2 つのアクティブ VLAN、Security Plus ライセンスで 3 つのアクティブ VLAN を設定でき、そのうちの 1 つはフェールオーバー用である必要があります。

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで最大 3 つのアクティブ VLAN、Security Plus ライセンスで最大 20 のアクティブ VLAN を設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

switchport access vlan コマンドを使用して、1 つ以上の物理インターフェイスを各 VLAN に割り当てることができます。デフォルトでは、インターフェイスの VLAN モードはアクセス ポートになります（インターフェイスに関連付けられた 1 つの VLAN）。インターフェイスで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode access trunk** コマンドを使用してモードをトランク モードに変更してから、**switchport trunk allowed vlan** コマンドを使用します。

例

次に、5 つの物理インターフェイスを 3 つの VLAN インターフェイスに割り当てる例を示します。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用して、VLAN モードをアクセス（デフォルト）またはトランクに設定します。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

構文の説明

access	スイッチ ポートをアクセス モードに設定します。このモードでは、スイッチ ポートで 1 つの VLAN のみのトラフィックを渡すことができます。パケットは、802.1Q VLAN タグなしでスイッチ ポートから出ます。パケットがタグ付きでスイッチ ポートに入ると、パケットはドロップされます。
trunk	スイッチ ポートをトランク モードに設定します。そのため、複数の VLAN のトラフィックを渡すことができます。パケットは、802.1Q VLAN タグ付きでスイッチ ポートから出ます。パケットがタグなしでスイッチ ポートに入ると、パケットはドロップされます。

デフォルト

デフォルトでは、モードはアクセスです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	1 つのトランクに制限されず、複数のトランク ポートを設定できるようになりました。

使用上のガイドライン

デフォルトでは、スイッチ ポートの VLAN モードはアクセス ポートになります（スイッチ ポートに関連付けられた 1 つの VLAN）。アクセス モードでは、**switchport access vlan** コマンドを使用してスイッチ ポートを VLAN に割り当てます。スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、モードをトランク モードに設定してから、**switchport trunk allowed vlan** コマンドを使用して複数の VLAN をトランクに割り当てます。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。

モードをアクセス モードに設定しない限り、**switchport vlan access** コマンドは有効になりません。モードをトランク モードに設定しない限り、**switchport trunk allowed vlan** コマンドは有効になりません。

例

次に、VLAN 100 に割り当てられたアクセス モードのスイッチ ポートおよび VLAN 200 および 300 に割り当てられたトランク モードのスイッチ ポートを設定する例を示します。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200,300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport monitor

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport monitor** コマンドを使用して、SPAN（スイッチ ポート モニタリングとも呼ばれる）をイネーブルにします。このコマンドを入力する対象のポート（宛先ポートと呼ばれる）では、指定した送信元ポートで送受信されるすべてのパケットのコピーを受信します。SPAN 機能を使用すると、トラフィックをモニタできるように、スニファを宛先ポートに接続できます。このコマンドを複数回入力して、複数の送信元ポートを指定できます。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。送信元ポートのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

構文の説明

source_port	モニタするポートを指定します。任意のイーサネット ポートおよび VLAN インターフェイス間でトラフィックを渡す Internal-Data0/1 バックプレーン ポートを指定できます。Internal-Data0/1 ポートはギガビット イーサネット ポートであるため、ファスト イーサネット宛先ポートをトラフィックによって過負荷にする場合があります。Internal-Data0/1 ポートは注意してモニタしてください。
tx	（任意）送信トラフィックのみをモニタすることを指定します。
rx	（任意）受信トラフィックのみをモニタすることを指定します。
both	（任意）送信トラフィックと受信トラフィックの両方をモニタすることを指定します。**both** がデフォルトです。

デフォルト

モニタするトラフィックのデフォルトのタイプは **both** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SPAN をイネーブルにしない場合、スニファをスイッチ ポートの 1 つに接続すると、そのポートで送受信されるトラフィックのみがキャプチャされます。複数のポートで送受信されるトラフィックをキャプチャするには、SPAN をイネーブルにし、モニタするポートを指定する必要があります。

ネットワーク ループになる可能性があるため、SPAN 宛先ポートを別のスイッチに接続するときは注意してください。

例

次に、イーサネット 0/0 ポートとイーサネット 0/2 ポートをモニタする宛先ポートとして、イーサネット 0/1 ポートを設定する例を示します。

```
hostname(config)# interface ethernet 0/1
hostname(config-if)# switchport monitor ethernet 0/0
hostname(config-if)# switchport monitor ethernet 0/2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

switchport protected

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport protected** コマンドを使用して、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信しないようにします。この機能により、あるスイッチ ポートが侵害された場合に、VLAN 上の他のスイッチ ポートに対して強固なセキュリティを提供します。

switchport protected

no switchport protected

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、インターフェイスは保護されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

保護されていないポートとの通信は、このコマンドによって制限されません。

例

次に、7 つのスイッチ ポートを設定する例を示します。イーサネット 0/4、0/5、および 0/6 は DMZ ネットワークに割り当てられ、相互から保護されます。

```
hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/5
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/6
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport trunk

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用して、VLAN をトランク ポートに割り当てます。VLAN をトランクから削除するには、このコマンドの **no** 形式を使用します。

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

構文の説明

allowed vlans *vlan_range*	トランク ポートに割り当てることができる 1 つ以上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4090 です。 *vlan_range* は、次のいずれかの方法で指定できます。 • 単一の番号（n） • 範囲（n-x） 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。 このコマンドにネイティブ VLAN を含めることができますが、必須ではありません。ネイティブ VLAN は、このコマンドに含まれているかどうかに関係なく渡されます。
native vlan *vlan*	ネイティブ VLAN をトランクに割り当てます。ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。 たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入るフレームで 802.1Q ヘッダーがないものは、VLAN 2 に渡されます。 各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

デフォルト

デフォルトでは、VLAN はトランクに割り当てられていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	このコマンドは、スイッチ ポートごとに 4 つ以上の VLAN を許可するように変更されました。また、1 つのみに制限されず、複数のトランク ポートを設定できるようになりました。このコマンドで、VLAN ID を区切るためにスペースではなくカンマも使用されます。
7.2(4)/8.0(4)	**native vlan** キーワードを使用するネイティブ VLAN サポートが追加されました。

使用上のガイドライン

スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode trunk** コマンドを使用してモードをトランク モードに設定してから、**switchport trunk** コマンドを使用して VLAN をトランクに割り当てます。このスイッチ ポートに少なくとも 1 つの VLAN を割り当てるまで、このスイッチ ポートでトラフィックを渡すことはできません。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。**switchport mode trunk** コマンドを使用してモードをトランク モードに設定しない限り、**switchport trunk** コマンドは有効になりません。

（注） このコマンドにはバージョン 7.2(1) との下位互換性はありません。VLAN を区切るカンマは 7.2(1) では認識されません。ダウングレードする場合は、VLAN をスペースで区切り、3 つの VLAN という制限を超えないようにしてください。

例

次に、7 つの VLAN インターフェイスを設定する例を示します。**failover lan** コマンドを使用して設定するフェールオーバー インターフェイスが含まれています。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

synack-data

データが含まれる TCP SYNACK パケットのアクションを設定するには、tcp マップ コンフィギュレーション モードで **synack-data** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

synack-data {**allow** | **drop**}

no synack-data

構文の説明

allow	データが含まれる TCP SYNACK パケットを許可します。
drop	データが含まれる TCP SYNACK パケットをドロップします。

デフォルト

デフォルト アクションでは、データが含まれる TCP SYNACK パケットをドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **synack-data**：tcp マップ コンフィギュレーション モードでは、**synack-data** などの数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、データが含まれる TCP SYNACK パケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# synack-data allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

syn-data

データが含まれる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

構文の説明

allow	データが含まれる SYN パケットを許可します。
drop	データが含まれる SYN パケットをドロップします。

デフォルト

デフォルトでは、SYN データが含まれるパケットは許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、SYN パケット内にデータが含まれるパケットをドロップします。

TCP の仕様によると、TCP 実装は SYN パケット内に含まれているデータを受け入れる必要があります。これは微妙であいまいな点であるため、一部の実装ではこのことが正しく処理されない場合があります。不適切なエンドシステム実装などの挿入攻撃に対する脆弱性を回避するために、SYN パケット内にデータが含まれるパケットをドロップすることを選択できます。

例

次に、データが含まれる SYN パケットをすべての TCP フローでドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
```

```
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

sysopt connection permit-vpn

VPN トンネルを介してセキュリティ アプライアンスに入り復号化されるトラフィックに対して、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用して、トラフィックがインターフェイス アクセス リストをバイパスできるようにします。グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection permit-vpn

no sysopt connection permit-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、デフォルトでイネーブルになりました。また、インターフェイス アクセス リストのみがバイパスされます。グループ ポリシーまたはユーザ単位のアクセス リストは有効なままです。
7.1(1)	このコマンドは、**sysopt connection permit-ipsec** から変更されました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスによって、VPN トラフィックがセキュリティ アプライアンスのインターフェイスで終端することが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、セキュリティ アプライアンスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます （グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます）。

no sysopt connection permit-vpn コマンドを入力して、インターフェイス アクセス リストをローカル IP アドレスに適用できます。アクセス リストを作成してインターフェイスに適用するには、**access-list** コマンドおよび **access-group** コマンドを参照してください。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。

例

次に、復号化された VPN トラフィックがインターフェイス アクセス リストに従うようにする例を示します。

```
hostname(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection preserve-vpn-flows

トンネルのドロップおよび回復後のタイムアウト期間内に、ステートフル（TCP）トンネル IPSec LAN-to-LAN トラフィックを保持して再開するには、**sysopt connection preserve-vpn-flows** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

永続的 IPSec トンネル フロー機能がイネーブルの場合、タイムアウト ウィンドウ内にトンネルが再作成される限り、セキュリティ アプライアンスで元のフロー内の状態情報にアクセスできるため、データは正常に流れ続けます。

このコマンドでは、ネットワーク拡張モードを含め、IPSec LAN-to-LAN トンネルのみがサポートされます。AnyConnect/SSL VPN または IPSec リモートアクセス トンネルはサポートされません。

例

次に、トンネルがドロップされ、タイムアウト期間内に再確立された後、トンネルの状態情報が保持されてトンネル IPSec LAN-to-LAN VPN トラフィックが再開されることを指定する例を示します。

```
hostname(config)# no sysopt connection preserve-vpn-flows
```

この機能がイネーブルかどうかを確認するには、sysopt に対して show run all コマンドを入力します。

```
hostname(config)# show run all sysopt
```

結果の例は次のとおりです。説明のために、これ以降のすべての例では、preserve-vpn-flows の項目は太字になっています。

```
no sysopt connection timewait
sysopt connection tcpmss 1380
```

```
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

既存の VPN フローを再分類するには、グローバル コンフィギュレーション モードで **sysopt connection reclassify-vpn** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

VPN トンネルがアップになると、このコマンドによって既存の VPN フローは再分類され、暗号化が必要なフローは分解されて再作成されます。

このコマンドは、LAN-to-LAN およびダイナミック VPN についてのみ適用されます。このコマンドは EZVPN または VPN クライアント接続には影響しません。

例

次に、VPN 再分類をイネーブルにする例を示します。

```
hostname(config)# sysopt connection reclassify-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-vpn	インターフェイスのアクセス リストをチェックすることなく、IPSec トンネルから受信するすべてのパケットを許可します。

コマンド	説明
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

最大 TCP セグメント サイズが設定した値を超えないようにし、指定したサイズ未満にならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

構文の説明

bytes	最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、*bytes* を 0 に設定します。 **minimum** キーワードの場合、*bytes* は許可される最も小さい最大値を表します。
minimum	最大セグメント サイズを上書きし、*bytes* 未満にならないようにします（48 ～ 65535 バイト）。この機能は、デフォルトでディセーブルです（0 に設定）。

デフォルト

デフォルトの最大値は 1380 バイトです。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。いずれかの最大が **sysopt connection tcpmss** コマンドで設定した値を超えている場合、セキュリティ アプライアンスによって最大は上書きされ、設定した値が挿入されます。いずれかの最大が **sysopt connection tcpmss minimum** コマンドで設定した値よりも小さい場合、セキュリティ アプライアンスによって最大は上書きされ、設定した「minimum」値が挿入されます（minimum 値は、実際には許可される最も小さい最大です）。たとえば、最大サイズを 1200 バイト、最小サイズを 400 バイトに設定した場合、ホストによって最大サイズ 1300 バイトが要求されると、セキュリティ アプライアンスによってパケットは 1200 バイト（最大）を要求するように変更されます。別のホストによって最大値 300 バイトが要求されると、セキュリティ アプライアンスによってパケットは 400 バイト（最小）を要求するように変更されます。

デフォルトの 1380 バイトでは、ヘッダー情報用の余地があるため、パケット サイズの合計は 1500 バイト（イーサネットのデフォルト MTU）を超えません。次の計算を参照してください。

1380 データ + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 バイト

ホストまたはサーバによって最大セグメント サイズが要求されない場合、セキュリティ アプライアンスでは RFC 793 のデフォルト値である 536 バイトが有効と見なされます。

1380 よりも大きい最大サイズを設定した場合、MTU サイズ（デフォルトでは 1500 バイト）によっては、パケットがフラグメント化される場合があります。フラグメントの数が多くなると、セキュリティ アプライアンスが Frag Guard 機能を使用する場合にパフォーマンスに影響を及ぼすことがあります。最小サイズを設定すると、TCP サーバから多数の小さい TCP データ パケットがクライアントに送信されることによってサーバおよびネットワークのパフォーマンスに影響を及ぼすことを防止できます。

（注） この機能の通常の使用には推奨されませんが、syslog IPFRAG メッセージ 209001 および 209002 が発生した場合は、*bytes* 値を大きくすることができます。

例

次に、最大サイズを 1200 に、最小サイズを 400 に設定する例を示します。

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

各 TCP 接続において、最後の通常の TCP クローズ ダウン シーケンスの後に、少なくとも 15 秒の短い TIME_WAIT 状態が強制的に維持されるようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。

sysopt connection timewait

no sysopt connection timewait

（注） RST パケット（通常の TCP クローズ ダウン シーケンスではない）でも、15 秒の遅延がトリガーされます。セキュリティ アプライアンスでは、接続の最後のパケット（FIN/ACK または RST）を受信した後、接続を 15 秒間保持します。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスでは、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放によって接続の一方の側で CLOSING 状態が保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスが完了するためのウィンドウが作成されます。

例

次に、timewait 機能をイネーブルにする例を示します。

```
hostname(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。

sysopt nodnsalias

alias コマンドを使用するときに DNS A レコード アドレスを変更する DNS インスペクションをディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt nodnsalias** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**alias** コマンドで NAT のみを実行し、DNS パケットの変更が不要な場合に、DNS アプリケーション インスペクションをディセーブルにします。

sysopt nodnsalias {**inbound** | **outbound**}

no sysopt nodnsalias {**inbound** | **outbound**}

構文の説明

inbound	セキュリティの低いインターフェイスから **alias** コマンドで指定されるセキュリティの高いインターフェイスへのパケットの DNS レコードの変更をディセーブルにします。
outbound	**alias** コマンドで指定されるセキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのパケットの DNS レコードの変更をディセーブルにします。

デフォルト

この機能は、デフォルトでディセーブルです（DNS レコード アドレス変更はイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

alias コマンドによって、NAT および DNS A レコード アドレスの変更が実行されます。DNS レコードの変更をディセーブルにする場合があります。

例

次に、着信パケットの DNS アドレスの変更をディセーブルにする例を示します。

```
hostname(config)# sysopt nodnsalias inbound
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt noproxyarp	インターフェイスでプロキシ ARP をディセーブルにします。

sysopt noproxyarp

インターフェイスで NAT グローバル アドレスまたは VPN クライアント アドレスに対するプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。プロキシ ARP を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

構文の説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

プロキシ ARP は、デフォルトでイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドは、VPN クライアント アドレスが内部ネットワークと重複するときに、VPN プロキシ ARP に影響を及ぼすように拡張されました。

使用上のガイドライン

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、セキュリティ アプライアンスは、デフォルトにより、すべてのインターフェイス上でプロキシ ARP を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP が不要なインターフェイスに対して **sysopt noproxyarp** コマンドを入力する必要があります。

まれに、NAT グローバル アドレスに対してプロキシ ARP をディセーブルにする場合があります。

ホストによって IP トラフィックが同じイーサネット ネットワーク上の別のデバイスに送信される場合、ホストではそのデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが IP アドレスを所有していなくても、その固有の MAC アドレスで ARP 要求に応答する場合に使用します。NAT を設定し、セキュリティ アプライアンスのインターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、セキュリティ アプライアンスによっ

てプロキシ ARP が使用されます。トラフィックがホストにアクセスできる唯一の方法は、セキュリティ アプライアンスでプロキシ ARP が使用されている場合、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次に、内部インターフェイスでプロキシ ARP をディセーブルにする例を示します。

```
hostname(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答内の認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。一部の RADIUS サーバとの互換性のために、このキーを無視する必要がある場合があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

一部の RADIUS サーバでは、アカウンティング確認応答内のオーセンティケータ ハッシュにこのキーが含まれていません。この使用上の注意により、セキュリティ アプライアンスでアカウンティング要求を継続的に再送信する場合があります。**sysopt radius ignore-secret** コマンドを使用して、これらの確認応答内のキーを無視し、再送信の問題を回避します （ここで示すキーは、**aaa-server host** コマンドで設定するものと同じです)。

例

次に、アカウンティング応答内の認証キーを無視する例を示します。

```
hostname(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。

CHAPTER 32

tcp-map コマンド～ type echo コマンド

tcp-map

一連の TCP 正規化アクションを定義するには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP 正規化機能によって、異常なパケットを識別する基準を指定できます。セキュリティ アプライアンスは、異常なパケットが検出されるとそれらをドロップします。TCP マップを削除するには、このコマンドの **no** 形式を使用します。

tcp-map *map_name*

no tcp-map *map_name*

構文の説明

map_name	TCP マップ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この機能は モジュラ ポリシー フレームワーク を使用します。最初に、**tcp-map** コマンドを使用して実行する TCP 正規化アクションを定義します。**tcp-map** コマンドによって、tcp マップ コンフィギュレーション モードが開始されます。このモードで、1 つ以上のコマンドを入力して、TCP 正規化アクションを定義できます。その後、**class-map** コマンドを使用して、TCP マップを適用するトラフィックを定義します。**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラスマップを参照します。クラス コンフィギュレーション モードで、**set connection advanced-options** コマンドを入力して TCP マップを参照します。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

次のコマンドは、tcp マップ コンフィギュレーション モードで使用可能です。

check-retransmission	再送信データのチェックをイネーブルまたはディセーブルにします。
checksum-verification	チェックサムの検証をイネーブルまたはディセーブルにします。
exceed-mss	ピアによって設定された MSS を超えるパケットを許可またはドロップします。

queue-limit	TCP 接続のキューに入れることができる順序が不正なパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズセキュリティ アプライアンスでのみ使用可能です。PIX 500 シリーズセキュリティ アプライアンスではキュー制限は 3 で、この値は変更できません。
reserved-bits	セキュリティ アプライアンスに予約済みフラグ ポリシーを設定します。
syn-data	データを持つ SYN パケットを許可またはドロップします。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。
ttl-evasion-protection	セキュリティ アプライアンスによって提供された TTL 回避保護をイネーブルまたはディセーブルにします。
urgent-flag	セキュリティ アプライアンスを通じて URG ポインタを許可またはクリアします。
window-variation	予期せずウィンドウ サイズが変更された接続をドロップします。

例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow

hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet

hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap

hostname(config-pmap-c)# service-policy pmap global
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類に使用するクラス マップを指定します。
clear configure tcp-map	TCP マップのコンフィギュレーションをクリアします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。

tcp-options

セキュリティ アプライアンスを通じて TCP オプションを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

no tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

tcp-options range *lower upper* {**allow** | **clear** | **drop**}

no tcp-options range *lower upper* {**allow** | **clear** | **drop**}

構文の説明

allow	TCP ノーマライザを介して TCP オプションを許可します。
clear	TCP ノーマライザを介して TCP オプションをクリアし、パケットを許可します。
drop	パケットをドロップします。
lower	下位バインド範囲（6 ～ 7）および（9 ～ 255）。
selective-ack	選択的確認応答メカニズム（SACK）オプションを設定します。デフォルトでは、SACK オプションを許可します。
timestamp	タイムスタンプ オプションを設定します。タイムスタンプ オプションをクリアすると、PAWS と RTT がディセーブルになります。デフォルトでは、タイムスタンプ オプションを許可します。
upper	上位バインド範囲（6 ～ 7）および（9 ～ 255）。
window-scale	ウィンドウ スケール メカニズム オプションを設定します。デフォルトでは、ウィンドウ スケール メカニズム オプションを許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。selective-acknowledgement、window-scale、および timestamp TCP オプションをクリアするには、tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用します。明確に定義されていないオプションを持つパケットをクリアまたはドロップすることもできます。

例

次に、6 ～ 7 および 9 ～ 255 の範囲内の TCP オプションを持つすべてのパケットをドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# tcp-options range 6 7 drop
hostname(config-tcp-map)# tcp-options range 9 255 drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

telnet

コンソールへの Telnet アクセスを追加し、アイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。以前に設定した IP アドレスから Telnet アクセスを削除するには、このコマンドの **no** 形式を使用します。

telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

no telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

構文の説明

hostname	セキュリティ アプライアンスの Telnet コンソールにアクセス可能なホストの名前を指定します。
interface_name	Telnet を実行するネットワーク インターフェイスの名前を指定します。
IP_address	セキュリティ アプライアンスへのログインが認可されているホストまたはネットワークの IP アドレスを指定します。
IPv6_address	セキュリティ アプライアンスへのログインが認可されている IPv6 アドレスおよびプレフィックスを指定します。
mask	IP アドレスに関連付けられているネットマスクを指定します。
timeout *number*	セキュリティ アプライアンスによって閉じられるまで、Telnet セッションのアイドル状態が保持される分数。有効な値は、1 ～ 1440 分です。

デフォルト

デフォルトでは、Telnet セッションは、アイドル状態のまま 5 分経過するとセキュリティ アプライアンスによって閉じられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	変数 *IPv6_address* が追加されました。**no telnet timeout** コマンドも追加されました。

使用上のガイドライン

telnet コマンドを使用すると、どのホストが Telnet を使用してセキュリティ アプライアンス コンソールにアクセスできるかを指定できます。すべてのインターフェイスでセキュリティ アプライアンスへの Telnet をイネーブルにすることができます。ただし、セキュリティ アプライアンスは、すべての Telnet トラフィックを IPSec で保護された外部インターフェイスへ強制的に転送します。外部インター

フェイスへの Telnet セッションをイネーブルにするには、セキュリティ アプライアンスによって生成された IP トラフィックを外部インターフェイスの IPSec に含めるように設定し、外部インターフェイスの Telnet をイネーブルにします。

以前に設定した IP アドレスから Telnet アクセスを削除するには、**no telnet** コマンドを使用します。**telnet timeout** コマンドを使用して、コンソール Telnet セッションが、セキュリティ アプライアンスによってログオフされるまでアイドル状態を継続できる最長時間を設定できます。**no telnet** コマンドは **telnet timeout** コマンドと一緒には使用できません。

IP アドレスを入力する場合は、ネットマスクも入力する必要があります。デフォルトのネットマスクはありません。内部ネットワークのサブネットワーク マスクは使用しないでください。*netmask* は IP アドレスのビット マスクのみです。単一の IP アドレスへのアクセスを制限するには、各オクテットで 255 を使用します。たとえば、255.255.255.255 です。

IPSec が動作している場合は、セキュアでないインターフェイス名（通常、これは外部インターフェイス）を指定できます。少なくとも、**crypto map** コマンドを設定して、**telnet** コマンドで使用するインターフェイス名を指定します。

passwd コマンドを使用して、コンソールへの Telnet アクセスのパスワードを設定できます。デフォルトは **cisco** です。**who** コマンドを使用して、現在、セキュリティ アプライアンス コンソールにアクセス中の IP アドレスを表示できます。**kill** コマンドを使用すると、アクティブ Telnet コンソール セッションを終了できます。

console キーワードを指定して **aaa** コマンドを使用する場合は、Telnet コンソール アクセスを認証サーバで認証する必要があります。

（注） セキュリティ アプライアンス Telnet コンソール アクセスの認証を要求するための **aaa** コマンドが設定されているときに、コンソール ログイン要求がタイムアウトした場合は、**enable password** コマンドで設定したセキュリティ アプライアンスのユーザ名とパスワードを入力することで、シリアル コンソールからセキュリティ アプライアンスへアクセスできるようになります。

例

次に、ホスト 192.168.1.3 と 192.168.1.4 に Telnet を介したセキュリティ アプライアンス コンソールへのアクセスを許可する例を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストにアクセス権が付与されています。

```
hostname(config)# telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# telnet 192.168.1.4 255.255.255.255 inside
hostname(config)# telnet 192.168.2.0 255.255.255.0 inside
hostname(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

次に、セッションの最大アイドル時間を変更する例を示します。

```
hostname(config)# telnet timeout 10
hostname(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

次に、Telnet コンソール ログイン セッションの例を示します（パスワードは、入力時に表示されません）。

```
hostname# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
hostname>
```

no telnet コマンドを使用して個々のエントリを、また、**clear configure telnet** コマンドを使用してすべての telnet コマンド ステートメントを削除できます。

```
hostname(config)# no telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
who	セキュリティ アプライアンス上のアクティブ Telnet 管理セッションを表示します。

terminal

現在の Telnet セッションでシステム ログ メッセージの表示を許可するには、特権 EXEC モードで **terminal monitor** コマンドを使用します。システム ログ メッセージをディセーブルにするには、**terminal no monitor** コマンドを使用します。

terminal {**monitor** | **no monitor**}

構文の説明

monitor	現在の Telnet セッションでシステム ログ メッセージの表示をイネーブルにします。
no monitor	現在の Telnet セッションでシステム ログ メッセージの表示をディセーブルにします。

デフォルト

システム ログ メッセージは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、システム ログ メッセージを表示し、現在のセッションでシステム ログ メッセージをディセーブルにする例を示します。

```
hostname# terminal monitor
hostname# terminal no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

構文の説明

[**lines**] *lines*	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在の Telnet セッションのみを対象に、pager line 設定を変更します。新しいデフォルトの pager 設定をコンフィギュレーションに保存するには、**pager** コマンドを使用します。

管理コンテキストに対して Telnet 接続し、他のコンテキストに変更した場合、そのコンテキストの **pager** コマンドで別の設定が使用される場合でも、pager line 設定はセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次に、表示される行数を 20 に変更する例を示します。

```
hostname# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。

コマンド	説明
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージを Telnet セッションで表示できるようにします。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal width

コンソール セッションで情報を表示する幅を設定するには、グローバル コンフィギュレーション モードで **terminal width** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

terminal width *columns*

no terminal width *columns*

構文の説明

columns	端末の幅をカラム数で指定します。デフォルト値は 80 です。指定できる範囲は 40 ～ 511 です。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、端末の表示幅を 100 カラムにする例を示します。

```
hostname# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	端末回線パラメータを特権 EXEC モードで設定します。

test aaa-server

セキュリティ アプライアンスが特定の AAA サーバでユーザを認証または認可できるかどうかを確認するには、特権 EXEC モードで **test aaa-server** コマンドを使用します。セキュリティ アプライアンス上の不正なコンフィギュレーションが原因で AAA サーバに到達できない場合があります。また、限定されたネットワーク コンフィギュレーションやサーバのダウンタイムなどの他の理由で AAA サーバに到達できないこともあります。

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*]}

構文の説明

authentication	AAA サーバの認証機能をテストします。
authorization	AAA サーバのレガシー VPN 認可機能をテストします。
host *ip_address*	サーバの IP アドレスを指定します。コマンドで IP アドレスを指定しないと、入力を求めるプロンプトが表示されます。
password *password*	ユーザ パスワードを指定します。コマンドでパスワードを指定しないと、入力を求めるプロンプトが表示されます。
server_tag	**aaa-server** コマンドで設定した AAA サーバ タグを指定します。
username *username*	AAA サーバの設定をテストするために使用するアカウントのユーザ名を指定します。ユーザ名が AAA サーバに存在することを確認してください。存在しないと、テストは失敗します。コマンドでユーザ名を指定しないと、入力を求めるプロンプトが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

test aaa-server コマンドでは、セキュリティ アプライアンスが特定の AAA サーバを使用してユーザを認証できることと、ユーザを認可できる場合は、レガシー VPN 認可機能を確認できます。このコマンドを使用すると、認証または認可を試みる実際のユーザを持たない AAA サーバをテストできます。また、AAA 障害の原因が、AAA サーバ パラメータの設定ミス、AAA サーバへの接続問題、またはセキュリティ アプライアンス上のその他のコンフィギュレーション エラーのいずれによるものかを特定するうえで役立ちます。

例

次に、ホスト 192.168.3.4 に srvgrp1 という RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、さらに認証ポートを 1650 に設定する例を示します。AAA サーバ パラメータのセットアップの後の **test aaa-server** コマンドによって、認証テストがサーバに到達できなかったことが示されます。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

次に、正常な結果となった **test aaa-server** コマンドの出力例を示します。

```
hostname# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

関連コマンド

コマンド	説明
aaa authentication console	管理トラフィックの認証を設定します。
aaa authentication match	通過するトラフィックの認証を設定します。
aaa-server	AAA サーバ グループを作成します。
aaa-server host	AAA サーバをサーバ グループに追加します。

test dynamic-access-policy attributes

dap 属性モードを入力するには、特権 EXEC モードから
test dynamic-access-policy attributes コマンドを入力します。これにより、ユーザ属性とエンドポイント属性の値ペアを指定できます。

dynamic-access-policy attributes

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

この機能は、DAP レコードの作成を試みます。

例

次に、**attributes** コマンドの使用例を示します。

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
attribute	ユーザ属性値ペアを指定できる属性モードを開始します。
display	現在の属性リストを表示します。

test dynamic-access-policy execute

test regex

正規表現をテストするには、特権 EXEC モードで **test regex** コマンドを使用します。

test regex *input_text regular_expression*

構文の説明

input_text	正規表現と一致させるテキストを指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、**regex** コマンドを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

test regex コマンドは、正規表現が一致すべきものと一致するかどうかをテストします。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

例

次に、正規表現に対して入力テキストをテストする例を示します。

```
hostname# test regex farscape scape
INFO: Regular expression match succeeded.

hostname# test regex farscape scaper

INFO: Regular expression match failed.
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。

test sso-server

テスト用の認証要求で SSO サーバをテストするには、特権 EXEC モードで **test sso-server** コマンドを使用します。

test sso-server *server-name* **username** *user-name*

構文の説明

server-name	テストする SSO サーバの名前を指定します。
user-name	テストする SSO サーバのユーザの名前を指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn	•	—	•	—	—
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
グローバル コンフィギュレーション モード	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、さらに、認証要求に応答しているかどうかをテストします。

server-name 引数で指定された SSO サーバが見つからない場合は、次のエラーが表示されます。

```
ERROR: sso-server server-name does not exist
```

SSO サーバが見つかったが、*user-name* 引数で指定されたユーザが見つからない場合は、認証は拒否されます。

認証では、セキュリティ アプライアンスは SSO サーバへの WebVPN ユーザのプロキシとして動作します。セキュリティ アプライアンスは現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。このコマンドは SSO サーバの両タイプに適用されます。

例

次に、特権 EXEC モードを開始し、ユーザ名 Anyuser を使用して SSO サーバ my-sso-server をテストし、正常な結果を得た例を示します。

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
hostname#
```

次に、同じサーバだが、ユーザ Anotheruser でテストし、認識されず、認証が失敗した例を示します。

```
hostname# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
hostname#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

text-color

ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定するには、webvpn モードで **text-color** コマンドを使用します。テキストの色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの no 形式を使用します。

text-color [*black* | *white* | *auto***]**

no text-color

構文の説明

auto	secondary-color コマンドの設定に基づいて黒または白を選択します。つまり、2 番めの色が黒の場合、この値は白となります。
black	タイトルバーのテキストのデフォルト色は白です。
white	色を黒に変更できます。

デフォルト

タイトルバーのテキストのデフォルト色は白です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、タイトルバーのテキストの色を黒に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# text-color black
```

関連コマンド

コマンド	説明
secondary-text-color	WebVPN ログイン ページ、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定します。

tftp-server

configure net コマンドまたは **write net** コマンドで使用するデフォルトの TFTP サーバとパスおよびファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

構文の説明

interface_name	ゲートウェイ インターフェイス名を指定します。最高のセキュリティ インターフェイス以外のインターフェイスを指定した場合は、そのインターフェイスがセキュアではないことを示す警告メッセージが表示されます。
server	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
filename	パスとファイル名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	現在ではゲートウェイ インターフェイスが必要です。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** コマンドと **write net** コマンドの入力が容易になります。**configure net** コマンドまたは **write net** コマンドを入力するときに、**tftp-server** コマンドで指定した TFTP サーバを継承するか、または独自の値を指定できます。また、**tftp-server** コマンドのパスをそのまま継承したり、**tftp-server** コマンド値の末尾にパスとファイル名を追加したり、**tftp-server** コマンド値を上書きすることもできます。

セキュリティ アプライアンスがサポートする **tftp-server** コマンドは 1 つだけです。

例

次の例では、TFTP サーバを指定し、コンフィギュレーションを /temp/config/test_config ディレクトリから読み取る方法を示します。

```
hostname(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
hostname(config)# configure net
```

関連コマンド

コマンド	説明
configure net	指定した TFTP サーバとパスからコンフィギュレーションをロードします。
show running-config tftp-server	デフォルトの TFTP サーバ アドレスとコンフィギュレーション ファイルのディレクトリを表示します。

tftp-server address

クラスタ内の TFTP サーバを指定するには、電話プロキシ コンフィギュレーション モードで **tftp-server address** コマンドを使用します。電話プロキシ コンフィギュレーションから TFTP サーバを削除するには、このコマンドの **no** 形式を使用します。

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

構文の説明

ip_address	TFTP サーバのアドレスを指定します。
interface *interface*	TFTP サーバが存在するインターフェイスを指定します。これは、TFTP サーバの実アドレスにする必要があります。
port	（任意）これは、TFTP サーバが TFTP 要求をリッスンするポートです。デフォルトの TFTP ポート 69 でない場合に、設定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

電話プロキシには、少なくとも 1 つの CUCM TFTP サーバを設定する必要があります。電話プロキシに対して TFTP サーバを 5 つまで設定できます。

TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。TFTP サーバは、CUCM と同じインターフェイス上に存在している必要があります。

内部 IP アドレスを使用して TFTP サーバを作成し、TFTP サーバが存在するインターフェイスを指定します。

IP 電話で、TFTP サーバの IP アドレスを次のように設定する必要があります。

- NAT が TFTP サーバ用に設定されている場合は、TFTP サーバのグローバル IP アドレスを使用します。
- NAT が TFTP サーバ用に設定されていない場合は、TFTP サーバの内部 IP アドレスを使用します。

サービス ポリシーがグローバルに適用されている場合は、TFTP サーバが存在するインターフェイスを除くすべての入力インターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。サービス ポリシーが特定のインターフェイスに適用されている場合は、指定された電話プロキシ モジュールへのインターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。

NAT ルールを TFTP サーバに設定する場合は、分類ルールのインストール時に TFTP サーバのグローバル アドレスが使用されるように、サービス ポリシーを適用する前に、NAT ルールを設定する必要があります。

例

次に、**tftp-server address** コマンドを使用して、電話プロキシに対応する 2 つの TFTP サーバを設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

threat-detection basic-threat

基本的な脅威の検出をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection basic-threat** コマンドを使用します。基本的な脅威の検出をディセーブルにするには、このコマンドの **no** 形式を使用します。

threat-detection basic-threat

no threat-detection basic-threat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

基本脅威検出は、デフォルトでイネーブルになっています。次のデフォルトのレート制限が使用されます。

表 32-1　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 400 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 320 秒間で 60 ドロップ / 秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
	直前の 3600 秒間で 4 ドロップ / 秒。	直近の 60 秒間で 8 ドロップ / 秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 200 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 60 秒間で 160 ドロップ / 秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 800 ドロップ / 秒。
	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 640 ドロップ / 秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 1600 ドロップ / 秒。
	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 1280 ドロップ / 秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ / 秒。	直前の 10 秒間で 8000 ドロップ / 秒。
	直前の 3600 秒間で 1600 ドロップ / 秒。	直近の 60 秒間で 6400 ドロップ / 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

基本的な脅威の検出をイネーブルにすると、セキュリティ アプライアンスは、次の理由によるドロップ パケットとセキュリティ イベントのレートをモニタします。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。完全なスキャンによる脅威の検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レート情報を使用し、ホストを攻撃者として分類してそれらのホストを自動的に回避するなどして対処します）。
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）

セキュリティ アプライアンスは、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

「デフォルト」の項の表 32-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。**threat-detection rate** コマンドを使用して、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。受信するイベントごとに、セキュリ

ティ アプライアンスは平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスはバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにする場合は、グローバル コンフィギュレーション モードで **threat-detection rate** コマンドを使用して、各イベント タイプのデフォルトのレート制限を変更できます。**threat-detection scanning-threat** コマンドを使用してスキャンによる脅威の検出をイネーブルにする場合は、このコマンドに **scanning-threat** キーワードを指定して、ホストを攻撃者またはターゲットと見なすタイミングを設定できます。設定しない場合は、基本的な脅威の検出とスキャンによる脅威の検出の両方で、デフォルトの **scanning-threat** 値が使用されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

構文の説明

acl-drop	アクセス リストによる拒否のためにドロップされたパケットのレート制限を設定します。
average-rate *av_rate*	平均レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。
bad-packet-drop	パケット形式に誤りがあって（invalid-ip-header や invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレート制限を設定します。
burst-rate *burst_rate*	バースト レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。バースト レートは、*N* 秒ごとの平均レートとして計算されます。*N* はバースト レート間隔です。バースト レート間隔は、**rate-interval** *rate_interval* 値の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。
conn-limit-drop	接続制限（システム全体のリソース制限とコンフィギュレーションで設定される制限の両方）を超えたためにドロップされたパケットのレート制限を設定します。
dos-drop	DoS 攻撃（無効な SPI、ステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレート制限を設定します。
fw-drop	基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレート制限を設定します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	不審な ICMP パケットが検出されたためにドロップされたパケットのレート制限を設定します。
inspect-drop	パケットがアプリケーション インスペクションに失敗したためにドロップされたパケットのレート制限を設定します。
interface-drop	インターフェイスの過負荷が原因でドロップされたパケットのレート制限を設定します。
rate-interval *rate_interval*	平均レート間隔を 600 ～ 2592000 秒（30 日）の範囲で設定します。レート間隔は、ドロップ数の平均値を求める期間を決定するために使用されます。また、バーストしきい値レート間隔を決定します。

scanning-threat	スキャン攻撃が検出されたためにドロップされたパケットのレート制限を設定します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	TCP SYN 攻撃やデータなし UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレート制限を設定します。

デフォルト

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、次のデフォルトのレート制限が使用されます。

表 32-2　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 400 ドロップ / 秒。
	直前の 3600 秒間で 100 ドロップ / 秒。	直近の 60 秒間で 400 ドロップ / 秒。
scanning-threat	直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
	直前の 3600 秒間で 5 ドロップ / 秒。	直前の 60 秒間で 10 ドロップ / 秒。
syn-attack	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 200 ドロップ / 秒。
	直前の 3600 秒間で 100 ドロップ / 秒。	直近の 60 秒間で 200 ドロップ / 秒。
acl-drop	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 800 ドロップ / 秒。
	直前の 3600 秒間で 400 ドロップ / 秒。	直近の 60 秒間で 800 ドロップ / 秒。
• **fw-drop** • **inspect-drop**	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 1600 ドロップ / 秒。
	直前の 3600 秒間で 400 ドロップ / 秒。	直近の 60 秒間で 1600 ドロップ / 秒。
interface-drop	直前の 600 秒間で 2000 ドロップ / 秒。	直前の 10 秒間で 8000 ドロップ / 秒。
	直近の 3600 秒間で 2000 ドロップ / 秒。	直近の 60 秒間で 8000 ドロップ / 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

基本的な脅威の検出をイネーブルにした場合、セキュリティ アプライアンスは、「構文の説明」の表で説明したイベント タイプによるドロップ パケットとセキュリティ イベントのレートをモニタします。

セキュリティ アプライアンスは、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

「デフォルト」の項の表 32-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。受信するイベントごとに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスはバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection scanning-threat

スキャンによる脅威の検出をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection scanning-threat** コマンドを使用します。スキャンによる脅威の検出をディセーブルにするには、このコマンドの **no** 形式を使用します。

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

構文の説明

duration *seconds*	攻撃元ホストの回避期間を 10 ～ 2592000 秒の範囲で設定します。デフォルトの期間は 3600 秒（1 時間）です。
except	IP アドレスを回避対象から除外します。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。
ip-address *ip_address mask*	回避対象から除外する IP アドレスを指定します。
object-group *network_object_group_id*	回避対象から除外するネットワーク オブジェクト グループを指定します。オブジェクト グループを作成するには、**object-group network** コマンドを参照してください。
shun	セキュリティ アプライアンスがホストを攻撃者と識別するとホスト接続を自動的に終了し、さらに、システム ログ メッセージ 733101 を送信します。

デフォルト

デフォルトの回避期間は 3600 秒（1 時間）です。

スキャン攻撃イベントでは、次のデフォルトのレート制限が使用されます。

表 32-3　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直前の 10 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直前の 60 秒間で 10 ドロップ/秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**duration** キーワードが追加されました。

使用上のガイドライン

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、セキュリティ アプライアンス のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

注意　スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、セキュリティ アプライアンスのパフォーマンスとメモリに大きく影響することがあります。

攻撃者に関するシステム ログ メッセージを送信するように セキュリティ アプライアンス を設定したり、自動的にホストを排除したりできます。デフォルトでは、ホストが攻撃者であると識別されると、システム ログ メッセージ 733101 が生成されます。

セキュリティ アプライアンスは、スキャンによる脅威イベント レートを超過した時点で、攻撃者とターゲットを識別します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。スキャン攻撃の一部と見なされるイベントが検出されるたびに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。スキャンによる脅威イベントのレート制限は **threat-detection rate scanning-threat** コマンドを使用して変更できます。

攻撃者またはターゲットとして分類されたホストを表示するには、**show threat-detection scanning-threat** コマンドを使用します。

回避対象のホストを表示するには、**show threat-detection shun** コマンドを使用します。排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、スキャンによる脅威の検出をイネーブルにし、10.1.1.0 ネットワーク上のホストを除き、攻撃者として分類されたホストを自動的に回避する例を示します。スキャンによる脅威の検出のデフォルトのレート制限は変更することもできます。

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

関連コマンド

コマンド	説明
clear threat-detection shun	ホストを回避対象から解除します。
show threat-detection scanning-threat	攻撃者およびターゲットとして分類されたホストを表示します。
show threat-detection shun	現在回避されているホストを表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。

threat-detection statistics

スキャンによる脅威の検出の統計情報をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection statistics** コマンドを使用します。スキャンによる脅威の検出の統計情報をディセーブルにするには、このコマンドの **no** 形式を使用します。

注意　統計情報をイネーブルにすると、イネーブルにした統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスに影響することがあります。**threat-detection statistics host** コマンドはパフォーマンスに大幅に影響を与えるため、トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討します。ただし、**threat-detection statistics port** コマンドは大きな影響を与えません。

threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

構文の説明

access-list	（任意）アクセス リストによる拒否の統計情報をイネーブルにします。アクセス リスト統計情報は、**show threat-detection top access-list** コマンドを使用した場合にだけ表示されます。
average-rate *attacks_per_sec*	（任意）TCP 代行受信について、syslog メッセージ生成の平均レートしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。
burst-rate *attacks_per_sec*	（任意）TCP 代行受信について、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
host	（任意）ホスト統計情報をイネーブルにします。ホスト統計情報は、ホストがアクティブであり、スキャン脅威ホスト データベース内にある間は蓄積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
port	（任意）ポート統計情報をイネーブルにします。
protocol	（任意）プロトコル統計情報をイネーブルにします。
rate-interval *minutes*	（任意）TCP 代行受信について、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間に、セキュリティ アプライアンスが攻撃をサンプリングする回数は 60 回です。
tcp-intercept	（任意）TCP 代行受信によって代行受信される攻撃の統計情報をイネーブルにします。TCP 代行受信をイネーブルにするには、**set connection embryonic-conn-max** コマンド、**nat** コマンド、または **static** コマンドを参照してください。

デフォルト

デフォルトでは、アクセス リスト統計情報はイネーブルです。このコマンドにオプションを指定しなかった場合は、すべてのオプションがイネーブルになります。

デフォルトの **tcp-intercept rate-interval** は 30 分です。デフォルトの **burst-rate** は 1 秒あたり 400 です。デフォルトの **average-rate** は 1 秒あたり 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。

使用上のガイドライン

統計情報を表示するには、**show threat-detection statistics** コマンドを使用します。

threat-detection scanning-threat コマンドを使用して、スキャンによる脅威の検出をイネーブルにする必要はありません。検出と統計情報は個別に設定できます。

例

次に、ホストを除くすべてのタイプのスキャンによる脅威の検出とスキャン脅威統計情報の例を示します。

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection statistics access-list
hostname(config)# threat-detection statistics port
hostname(config)# threat-detection statistics protocol
hostname(config)# threat-detection statistics tcp-intercept
```

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。

threshold

SLA モニタリング動作のしきい値超過イベントのしきい値を設定するには、SLA モニタ コンフィギュレーション モードで **threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

threshold *milliseconds*

no threshold

構文の説明

milliseconds	宣言する上昇しきい値をミリ秒で指定します。有効な値は、0 ～ 2147483647 です。この値は、タイムアウトに設定された値以下にする必要があります。

デフォルト

デフォルトのしきい値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

しきい値は、しきい値超過イベントを示すためにだけ使用されます。到達可能性には影響しませんが、**timeout** コマンドの適切な設定を評価するために使用できます。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

timeout

さまざまな機能に対応するグローバルな最大アイドル時間を設定するには、グローバル コンフィギュレーション モードで **timeout** コマンドを使用します。すべてのタイムアウトをデフォルトに戻すには、このコマンドの **no** 形式を使用します。単一の機能をデフォルトにリセットするには、**timeout** コマンドにデフォルト値を指定して再度入力します。

timeout {**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media** | **tcp-proxy-reassembly**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

構文の説明

absolute	（任意）uauth timeout が期限切れになった後、再認証を要求します。デフォルトでは、**absolute** キーワードはイネーブルです。非アクティブな状態が一定時間経過した後 uauth タイマーがタイムアウトするように設定するには、代わりに **inactivity** キーワードを入力します。
conn	（任意）接続を閉じた後のアイドル時間を 0:05:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
hh:*mm*:*ss*	タイムアウトを、時間、分、秒で指定します。接続をタイムアウトしない場合は、**0** を使用します（可能な場合）。
h225	（任意）H.225 シグナリング接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。タイムアウト値を 0:0:01 に指定すると、タイマーはディセーブルになり、TCP 接続はすべてのコールがクリアされるとすぐに切断されます。
h323	（任意）H.245（TCP）および H.323（UDP）メディア接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
half-closed	（任意）TCP half-closed 接続を解放するまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
icmp	（任意）ICMP のアイドル時間を 0:0:02 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 秒（0:0:02）です。
inactivity	（任意）非アクティブ タイムアウトが期限切れになった後、uauth 再認証を要求します。
mgcp	（任意）MGCP メディア接続を削除するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは、5 分（0:5:0）です。
mgcp-pat	（任意）MGCP PAT 変換を削除するまでの絶対間隔を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 5 分（0:5:0）です。
rpc	（任意）RPC スロットを解放するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、5 分（0:05:0）です。
sip	（任意）SIP 制御接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、30 分（0:30:0）です。接続がタイムアウトしないようにするには、**0** を使用します。

sip-disconnect	（任意）CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間を 0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sip-invite	（任意）暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、3 分（0:3:0）です。
sip_media	（任意）SIP メディア接続を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。 SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
sip-provisional-media	（任意）SIP プロビジョナル メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sunrpc	（任意）SUNRPC スロットを閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
tcp-proxy-reassembly	（任意）再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
uauth	（任意）認証および認可キャッシュがタイムアウトし、ユーザが次回接続時に再認証が必要となるまでの継続時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。デフォルトのタイマーは absolute です。**inactivity** キーワードを入力すると、無活動の期間後にタイムアウトが発生するように設定できます。**uauth** 継続時間は、**xlate** 継続時間より短く設定する必要があります。キャッシュをディセーブルにするには、**0** に設定します。接続に受動 FTP を使用している場合、または Web 認証に **virtual http** コマンドを使用している場合は、**0** を使用しないでください。
udp	（任意）UDP スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
xlate	（任意）変換スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 3 時間（3:0:0）です。

デフォルト

デフォルトの設定は次のとおりです。

- **conn** *hh*:*mm*:*ss* は 1 時間（**1:0:0**）です。
- **h225** *hh*:*mm*:*ss* は 1 時間（**1:0:0**）です。
- **h323** *hh*:*mm*:*ss* は 5 分（**0:5:0**）です。
- **half-closed** *hh*:*mm*:*ss* は 10 分（**0:10:0**）です。
- **icmp** *hh:mm:ss* は 2 秒（**0:0:2**）です。
- **mgcp** *hh:mm:ss* は 5 分（**0:5:0**）です。
- **mgcp-pat** *hh:mm:ss* は 5 分（**0:5:0**）です。
- **rpc** *hh*:*mm*:*ss* は 5 分（**0:5:0**）です。
- **sip** *hh:mm:* は 30 分（**0:30:0**）です。
- **sip-disconnect** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sip-invite** *hh:mm:ss* は 3 分（**0:3:0**）です。

- **sip_media** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sip-provisional-media** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sunrpc** *hh:mm:ss* は、10 分（**0:10:0**）です。
- **tcp-proxy-reassembly** *hh:mm:ss* は 1 分（**0:1:0**）です。
- **uauth** *hh:mm:ss* は 5 分（**00:5:00**）**絶対時間**です。
- **udp** *hh:mm:ss* は 2 分（**00:02:00**）です。
- **xlate** *hh*:*mm*:*ss* は 3 時間（**03:00:00**）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	**mgcp-pat**、**sip-disconnect**、および **sip-invite** キーワードが追加されました。
7.2(4)/8.0(4)	**sip-provisional-media** キーワードが追加されました。
7.2(5)/8.0(5)	**tcp-proxy-reassembly** キーワードが追加されました。

使用上のガイドライン

timeout コマンドを使用すると、グローバルにタイムアウトを設定できます。一部の機能では、コマンドで指定されたトラフィックに対し、**set connection timeout** コマンドが優先されます。

timeout コマンドの後に、キーワードと値を複数入力できます。

接続タイマー（**conn**）は変換タイマー（**xlate**）より優先されます。変換タイマーは、すべての接続がタイムアウトになった後にのみ動作します。

例

次に、最大アイドル時間を設定する例を示します。

```
hostname(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
hostname(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

関連コマンド

コマンド	説明
clear configure timeout	タイムアウト コンフィギュレーションをクリアし、デフォルトにリセットします。
set connection timeout	Modular Policy Framework を使用して接続タイムアウトを設定します。
show running-config timeout	指定されたプロトコルのタイムアウト値を表示します。

timeout（AAA サーバ ホスト）

AAA サーバとの接続確立を中断するまでに許容される、ホスト固有の最大応答時間を秒単位で設定するには、aaa サーバ ホスト モードで **timeout** コマンドを使用します。タイムアウト値を削除し、タイムアウトをデフォルト値の 10 秒にリセットするには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout

構文の説明

seconds	要求のタイムアウト間隔（1 ～ 60 秒）を指定します。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはすべての AAA サーバ プロトコル タイプで有効です。

セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。**retry-interval** コマンドを使用して、セキュリティ アプライアンスが各接続試行の間で待機する時間を指定できます。

タイムアウトは、セキュリティ アプライアンスがサーバとのトランザクションの完了を試みて費やす時間の合計です。再試行間隔は、タイムアウト期間中に通信を再試行する頻度を決定します。そのため、再試行間隔をタイムアウト値以上にすると、再試行は行われません。再試行が実行されるようにするには、再試行間隔をタイムアウト値より小さくする必要があります。

例

次に、ホスト 1.2.3.4 の RADIUS AAA サーバ「svrgrp1」が 30 秒のタイムアウト値と 10 秒の再試行間隔を使用するように設定する例を示します。セキュリティ アプライアンスは、30 秒後に通信試行を中断するまでに 3 回試行を繰り返します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
```

```
hostname(config-aaa-server-host)# timeout 30
hostname(config-aaa-server-host)# retry-interval 10
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa	現在の AAA コンフィギュレーションの値を表示します。

timeout（dns サーバ グループ コンフィギュレーション モード）

次の DNS サーバを試行するまでの待機時間の合計を指定するには、dns サーバ グループ コンフィギュレーション モードで **timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用して、再試行回数を設定できます。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、DNS サーバ グループ「dnsgroup1」のタイムアウトを 1 秒に設定する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns timeout 1
```

関連コマンド

コマンド	説明
clear configure dns	ユーザが作成した DNS サーバ グループをすべて削除し、デフォルト サーバ グループの属性をデフォルト値にリセットします。
domain-name	デフォルトのドメイン名を設定します。

コマンド	説明
retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

timeout（gtp マップ）

GTP セッションの非アクティブ タイマーを変更するには、**gtp-map** コマンドを使用してアクセスする GTP マップ コンフィギュレーション モードで **timeout** コマンドを使用します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

no timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。
gsn	GSN を削除するまでの非アクティブな期間を指定します。
pdp-context	PDP コンテキストの受信を開始する前に許容される最大時間を指定します。
request	GTP メッセージの受信を開始する前に許容される最大時間を指定します。
signaling	GTP シグナリングを削除するまでの非アクティブな期間を指定します。
t3-response	GTP 接続を削除する前に応答を待機する最大時間を指定します。
tunnel	GTP トンネルを切断するまでの非アクティブな期間を指定します。

デフォルト

gsn、**pdp-context**、および **signaling** のデフォルトは 30 分です。

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 時間です（PDP コンテキスト削除要求を受信しない場合）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル（PDP）コンテキストは、IMSI と NSAPI との組み合わせである Tunnel Identifier（TID; トンネル ID）によって識別されます。各 MS は最大 15 の NSAPI を保持できるため、多様な QoS レベルのアプリケーション要件に基づいて、それぞれ異なる NSAPI を持つ PDP コンテキストを複数作成できます。

GTP トンネルは、異なる GSN ノードにある 2 個の関連する PDP コンテキストによって定義され、1 つのトンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークとモバイル ステーション ユーザの間でパケットを転送するために必要です。

例

次に、要求キューのタイムアウト値を 2 分に設定する例を示します。

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# timeout request 00:02:00
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

timeout（RADIUS アカウンティング）

RADIUS アカウンティング ユーザの非アクティブ タイマーを変更するには、**inspect radius-accounting** コマンドを使用してアクセスする radius アカウンティング パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。デフォルトは 1 時間です。
users	ユーザのタイムアウトを指定します。

デフォルト

ユーザのデフォルトのタイムアウトは 1 時間です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
radius アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ユーザのタイムアウト値を 10 分に設定する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout user 00:10:00
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

timeout（sla モニタ）

SLA 動作が要求パケットへの応答を待機する時間を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで、**timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timeout *milliseconds*

no timeout

構文の説明

milliseconds	0 ～ 604800000

デフォルト

デフォルトのタイムアウト値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

frequency コマンドを使用して、SLA 動作が要求パケットを送信する頻度を設定し、**timeout** コマンドを使用して、SLA 動作がそれらの要求への応答の受信を待機する時間を設定できます。**timeout** コマンドには、**frequency** コマンドに指定する値より大きい値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
sla monitor	SLA モニタリング動作を定義します。

timeout pinhole

DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きするには、パラメータ コンフィギュレーション モードで **timeout pinhole** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

timeout pinhole *hh:mm:ss*

no timeout pinhole

構文の説明

hh:mm:ss	ピンホール接続のタイムアウト。指定できる値は 0:0:1 ～ 1193:0:0 です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、DCERPC インスペクション ポリシー マップでピンホール接続のピンホール タイムアウトを設定する例を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout pinhole 0:10:00
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

time-range

時間範囲コンフィギュレーション モードを開始し、トラフィック ルールにアタッチできる時間範囲、またはアクションを定義するには、グローバル コンフィギュレーション モードで **time-range** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

time-range *name*

no time-range *name*

構文の説明

name	時間範囲の名前。名前は 64 文字以下にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間範囲を作成してもデバイスへのアクセスは制限されません。**time-range** コマンドは時間範囲のみを定義します。時間範囲を定義した後、それをトラフィック ルールまたはアクションにアタッチできます。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

時間範囲はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次に、時間範囲「New_York_Minute」を作成し、時間範囲コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# time-range New_York_Minute
hostname(config-time-range)#
```

時間範囲を作成し、時間範囲コンフィギュレーション モードを開始した後、**absolute** コマンドと **periodic** コマンドを使用して時間範囲パラメータを定義できます。**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。その後、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

ACL の詳細については、**access-list extended** コマンドを参照してください。

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。

timeout secure-phones

電話プロキシ データベースからセキュア フォン エントリを削除するまでのアイドル タイムアウトを設定するには、電話プロキシ コンフィギュレーション モードで **timeout secure-phones** コマンドを使用します。タイムアウト値をデフォルトの 5 分に戻すには、このコマンドの **no** 形式を使用します。

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

構文の説明

hh:mm:ss	オブジェクトを削除するまでのアイドル タイムアウトを指定します。デフォルトは 5 分です。

デフォルト

セキュア フォン タイムアウトのデフォルト値は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。エントリのタイムスタンプは、電話プロキシが SIP 電話の登録更新および SCCP 電話のキープアライブを受信するたびに更新されます。

timeout secure-phones コマンドのデフォルト値は 5 分です。SCCP キープアライブおよび SIP レジスタ更新の最大タイムアウト値より大きい値を指定します。たとえば、SCCP キープアライブが 1 分間隔に指定され、SIP レジスタ更新が 3 分に設定されている場合は、このタイムアウト値には 3 分より大きい値を設定します。

例

次に、**timeout secure-phones** コマンドを使用して、電話プロキシが 3 分後にセキュア フォン データベースのエントリをタイムアウトにするように設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
```

```
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# timeout secure-phones 00:03:00
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

timers lsa-group-pacing

OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、ルータ コンフィギュレーション モードで **timers lsa-group-pacing** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

構文の説明

seconds	OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を変更するには **timers lsa-group-pacing** *seconds* コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers lsa-group-pacing** コマンドを使用します。

例

次に、LSA のグループ処理間隔を 500 秒に設定する例を示します。

```
hostname(config-router)# timers lsa-group-pacing 500
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
timers spf	Shortest Path First（SPF; 最短パス優先）計算遅延とホールド タイムを指定します。

timers spf

Shortest Path First（SPF; 最短パス優先）計算遅延とホールド タイムを指定するには、ルータ コンフィギュレーション モードで **timers spf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

構文の説明

delay	OSPF がトポロジ変更を受信してから Shortest Path First（SPF; 最短パス優先）計算を開始するまでの遅延時間を 1 ～ 65535 の範囲（秒単位）で指定します。
holdtime	2 つの連続する SPF 計算の間のホールド タイム（秒単位）。有効な値は、1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

- *delay* は 5 秒です。
- *holdtime* は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

OSPF プロトコルがトポロジ変更を受信してから計算を開始するまでの遅延時間と、2 つの連続する SPF 計算の間のホールド タイムを設定するには、**timers spf** コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers spf** コマンドを使用します。

例

次に、SPF 計算遅延を 10 秒に設定し、SPF 計算ホールド タイムを 20 秒に設定する例を示します。

```
hostname(config-router)# timers spf 10 20
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
timers lsa-group-pacing	OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

title

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示する WebVPN ページのタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **title** コマンドを使用します。

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「WebVPN Service」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

タイトルを付けない場合は、*value* 引数を指定せずに **title text** コマンドを使用します。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次の例では、タイトルがテキスト「Cisco WebVPN Service」でカスタマイズされています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
page style	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータを使用して WebVPN ページをカスタマイズします。

tls-proxy

TLS コンフィギュレーション モードで TLS プロキシ インスタンスを設定したり、最大セッション数を設定したりするには、グローバル コンフィギュレーション モードで **tls-proxy** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

構文の説明

max_sessions *max_sessions*	プラットフォームでサポートする TLS プロキシ セッションの最大数を指定します。
noconfirm	確認を要求せずに **tls-proxy** コマンドを実行します。
proxy_name	TLS プロキシ インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

tls-proxy コマンドを使用して TLS プロキシ コンフィギュレーション モードを開始し、TLS プロキシ インスタンスを作成したり、プラットフォームでサポートされる最大セッション数を設定したりできます。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。

tos

SLA 動作要求パケットの IP ヘッダー内のタイプ オブ サービス バイトを定義するには、SLA モニタ プロトコル コンフィギュレーション モードで **tos** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

tos *number*

no tos

構文の説明

number	IP ヘッダーで使用するサービス タイプの値。有効な値は、0 ～ 255 です。

デフォルト

デフォルトのタイプ オブ サービス値は 0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。これは、専用アクセス レートなどのポリシー ルーティングおよび機能のために、ネットワーク上の他のルータによって使用されます。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。エコー要求パケットのペイロード サイズを 48 バイトに設定し、SLA 動作中に送信されるエコー要求数を 5 に、さらにタイプ オブ サービス バイトを 80 に設定します。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# tos 80
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

traceroute

パケットが宛先に到達するまでにたどるルートを調査するには、**traceroute** コマンドを使用します。

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

構文の説明

destination_ip	traceroute の宛先 IP アドレスを指定します。
hostname	ルートをトレースする先のホストのホスト名。ホスト名を指定する場合は、**name** コマンドで定義するか、traceroute をイネーブルにしてホスト名を IP アドレスに解決するように DNS サーバを設定します。www.example.com などの DNS ドメイン名をサポートします。
source	トレース パケットの送信元として使用される IP アドレスまたはインターフェイスを指定します。
source_ip	パケット トレースの送信元 IP アドレスを指定します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードでは、セキュリティ アプライアンスの管理 IP アドレスにする必要があります。
source_interface	パケット トレースの送信元インターフェイスを指定します。指定する場合は、送信元インターフェイスの IP アドレスが使用されます。
numeric	出力に中間ゲートウェイの IP アドレスのみが示されるように指定します。このキーワードを指定しない場合は、トレース中に到達したゲートウェイのホスト名の検索を試みます。
timeout	使用されるタイムアウト値を指定します。
timeout_value	接続をタイムアウトにする前に応答を待機する時間を指定します。デフォルトは 3 秒です。
probe *probe_num*	TTL の各レベルで送信するプローブの数。デフォルト数は 3 です。
ttl	プローブで使用する存続可能時間の値の範囲を指定するキーワード。
min_ttl	最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホップの表示を抑制するためにより大きい値を設定できます。
max-ttl	使用可能な最大 TTL 値。デフォルト値は 30 です。traceroute パケットが宛先に到達するか、値に達したときにコマンドは終了します。
port *port_value*	ユーザ データグラム プロトコル（UDP）プローブ メッセージによって使用される宛先ポート。デフォルト値は 33434 です。
use-icmp	UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するように指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

traceroute コマンドは送信した各プローブの結果を示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次に、**traceroute** コマンドによって表示される出力記号を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

例

次に、宛先 IP アドレスを指定した場合の traceroute 出力の例を示します。

```
hostname# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
packet-tracer	パケット トレース機能をイネーブルにします。

track rtr

SLA 動作の到達可能性を追跡するには、グローバル コンフィギュレーション モードで **track rtr** コマンドを使用します。SLA 追跡を削除するには、このコマンドの **no** 形式を使用します。

track *track-id* **rtr** *sla-id* **reachabilitity**

no track *track-id* **rtr** *sla-id* **reachabilitity**

構文の説明

reachability	オブジェクトの到達可能性を追跡するように指定します。
sla-id	トラッキング エントリが使用する SLA の ID。
track-id	トラッキング エントリ オブジェクト ID を作成します。有効な値は、1 ～ 500 です。

デフォルト

SLA 追跡はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

track rtr コマンドは、トラッキング エントリ オブジェクト ID を作成し、トラッキング エントリが使用する SLA を指定します。

各 SLA 動作が、トラッキング プロセスによって解釈される動作戻りコード値を維持します。戻りコードには、OK や Over Threshold などのいくつかの戻りコードがあります。表 32-4 は、これらの戻りコードに関連するオブジェクトの到達可能性ステートを表示します。

表 32-4　SLA 追跡の戻りコード

トラッキング	戻りコード	追跡ステート
Reachability	OK または Over Threshold	Up
	他の任意のコード	Down

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
route	スタティック ルートを設定します。
sla monitor	SLA モニタリング動作を定義します。

traffic-non-sip

既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可するには、パラメータ コンフィギュレーション モードで **traffic-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

traffic-non-sip

no traffic-non-sip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# traffic-non-sip
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

transfer-encoding

転送エンコーディング タイプを指定して HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセス可能な HTTP マップ コンフィギュレーション モードで、**transfer-encoding** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	指定した転送エンコーディング タイプを使用する接続が検出されたときに実行するアクションを指定します。
allow	メッセージを許可します。
chunked	メッセージ本文を一連のチャンクとして転送する転送エンコーディング タイプを識別します。
compress	メッセージ本文を UNIX ファイル圧縮を使用して転送する転送エンコーディング タイプを識別します。
default	トラフィックが設定されたリストにないサポートされる要求方式を含む場合にセキュリティ アプライアンスが実行するデフォルトのアクションを指定します。
deflate	メッセージ本文を zlib 形式（RFC 1950）とデフレート圧縮（RFC 1951）を使用して転送する転送エンコーディング タイプを識別します。
drop	接続を閉じます。
gzip	メッセージ本文を GNU zip（RFC 1952）を使用して転送する転送エンコーディング タイプを識別します。
identity	転送エンコーディングが実行されていないメッセージ本文の接続を識別します。
log	（任意）syslog を生成します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。
type	HTTP アプリケーション インスペクションを通じて制御される転送エンコーディングのタイプを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。コマンドがイネーブルで、サポートされる転送エンコーディング タイプが指定されていない場合、デフォルト アクションでは、ロギングなしで接続を許可します。デフォルトのアクションを変更するには、**default** キーワードを使用して、別のデフォルト アクションを指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

transfer-encoding コマンドがイネーブルの場合、セキュリティ アプライアンスは、サポートされ設定されている各転送エンコーディング タイプの HTTP 接続に指定されたアクションを適用します。

セキュリティ アプライアンスは、設定されたリストの転送エンコーディング タイプに一致*しない*すべてのトラフィックに**デフォルト**のアクションを適用します。設定済みの**デフォルト**のアクションでは、ロギングなしで接続を**許可**します。

たとえば、設定済みのデフォルトのアクションでは、**drop** と **log** のアクションを伴う 1 つ以上のエンコーディング タイプを指定した場合、セキュリティ アプライアンスは、設定されたエンコーディング タイプを含む接続をドロップし、各接続をロギングし、その他のサポートされるエンコーディング タイプの接続をすべて許可します。

より限定的なポリシーを設定する場合は、デフォルトのアクションを **drop**（または **reset**）と **log**（イベントをロギングする場合）に変更します。その後、許可されたエンコーディング タイプそれぞれに **allow** アクションを設定します。

適用する各設定に対して 1 回ずつ **transfer-encoding** コマンドを入力します。デフォルト アクションを変更するために **transfer-encoding** コマンドの 1 つのインスタンスを使用し、設定された転送エンコーディング タイプのリストに各エンコーディング タイプを追加するために 1 つのインスタンスを使用します。

設定されたアプリケーション タイプのリストからアプリケーション カテゴリを削除するために、このコマンドの **no** 形式を使用する場合は、コマンドラインのアプリケーション カテゴリ キーワードの後ろの文字は無視されます。

例

次に、特に禁止されていないすべてのサポートされるアプリケーション タイプを許可する設定済みのデフォルトを使用して、許可ポリシーを提供する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# transfer-encoding gzip drop log
hostname(config-http-map)#
```

この場合、GNU zip を使用する接続だけがドロップされ、そのイベントがロギングされます。

次に、デフォルト アクションを、接続のリセットと、特に許可されていないすべてのエンコーディング タイプのロギングに変更した、限定的なポリシーを提供する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse identity allow
hostname(config-http-map)#
```

この場合、転送エンコーディングを使用していない接続だけが許可されます。他のサポートされるエンコーディング タイプの HTTP トラフィックを受信した場合は、セキュリティ アプライアンスは接続をリセットして syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

trust-point

IKE ピアに送信する証明書を識別するトラストポイントの名前を指定するには、トンネル グループ ipsec 属性モードで、**trust-point** コマンドを使用します。トラストポイントの指定を削除するには、このコマンドの **no** 形式を使用します。

trust-point *trust-point-name*

no trust-point *trust-point-name*

構文の説明

trust-point-name	使用するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

例

次に、設定 ipsec コンフィギュレーション モードを開始し、IPSec LAN-to-LAN トンネル グループ 209.165.200.225 の IKE ピアに送信される証明書を識別するためのトラストポイントを設定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

trustpoint（SSO サーバ）

SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントの名前を指定するには、config-webvpn-sso-saml モードで **trustpoint** コマンドを使用します。トラストポイントの指定を削除するには、このコマンドの **no** 形式を使用します。

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

構文の説明

trustpoint-name	使用するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-saml	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3	このコマンドが追加されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。

例

次に、config-webvpn-sso-saml モードを開始し、SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントに名前を付ける例を示します。

```
hostname(config-webvpn)# sso server
hostname(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント情報を管理します。
show webvpn sso server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso server	SSO サーバのタイプを作成、命名、および指定します。

tsig enforced

TSIG リソース レコードの存在を必須とするには、パラメータ コンフィギュレーション モードで **tsig enforced** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

構文の説明

drop	TSIG が存在しない場合にパケットをドロップします。
log	システム メッセージ ログを生成します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS トランザクションにおける TSIG の存在のモニタと強制をイネーブルにします。

例

次に、DNS インスペクション ポリシー マップ内で TSIG 強制をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tsig enforced action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

ttl-evasion-protection

存続可能時間回避保護をディセーブルにするには、tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

ttl-evasion-protection

no ttl-evasion-protection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

セキュリティ アプライアンスによって提供される TTL 回避保護は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用して、セキュリティ ポリシーを回避しようとする攻撃を阻止できます。

たとえば、攻撃者は非常に短い TTL を持ち、ポリシーに合致するパケットを送信できます。TTL がゼロになると、セキュリティ アプライアンスとエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、セキュリティ アプライアンスにとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。この機能をイネーブルにすると、このような攻撃を阻止します。

例

次に、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローに対して TTL 回避保護をディセーブルにする例を示します。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# ttl-evasion-protection disable
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

tunnel-group

IPSec および WebVPN トンネルの接続固有のデータベースを作成し管理するには、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを使用します。トンネル グループを削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **type** *type*

no tunnel-group *name*

構文の説明

name	トンネル グループの名前を指定します。任意のストリングを選択できます。名前が IP アドレスの場合は、通常、ピアの IP アドレスとなります。
type	トンネル グループのタイプを指定します。 • remote-access：ユーザに IPSec リモート アクセスまたは WebVPN（ポータルまたはトンネル クライアント）のいずれかを使用した接続を許可します。 • ipsec-l2l：2 つのサイトまたは LAN がインターネットなどのパブリック ネットワークを介してセキュアに接続できる IPsec LAN-to-LAN を指定します。 **（注）** 次のトンネル グループ タイプは、リリース 8.0(2) で廃止されました。 ipsec-ra：IPSec リモート アクセス webvpn：WebVPN セキュリティ アプライアンスはこれらを remote-access タイプに変換します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	「注」を参照してください。	•	—	—

（注） tunnel-group コマンドは、トランスペアレント ファイアウォール モードで使用可能です。このモードでは、LAN-to-LAN トンネル グループのコンフィギュレーションは設定できますが、remote-access グループまたは WebVPN グループの設定はできません。LAN-to-LAN に対応する tunnel-group コマンドはすべてトランスペアレント ファイアウォール モードで使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn タイプが追加されました。
8.0(2)	remote-access タイプが追加され、ipsec-ra タイプと webvpn タイプが廃止されました。

使用上のガイドライン

セキュリティ アプライアンスには、次のデフォルト トンネル グループがあります。

- DefaultRAGroup、デフォルトの IPSec remote-access トンネル グループ
- DefaultL2LGroup、デフォルトの IPSec LAN-to-LAN トンネル グループ
- DefaultWEBVPNGroup、デフォルトの WebVPN トンネル グループ

これらのグループは変更できますが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、セキュリティ アプライアンスは、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

tunnel-group コマンドを入力した後、適切な後続のコマンドを入力して、特定のトンネル グループの特定の属性を設定できます。これらのコマンドはそれぞれ、トンネル グループ属性を設定するためのコンフィギュレーション モードを開始します。

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

例

次に、グローバル コンフィギュレーション モードを開始する例を示します。最初に、リモート アクセス トンネル グループを設定します。グループ名は group1 です。

```
hostname(config)# tunnel-group group1 type remote-access
hostname(config)#
```

次に、webvpn トンネル グループ「group1」を設定する tunnel-group コマンドの例を示します。このコマンドはグローバル コンフィギュレーション モードで入力します。

```
hostname(config)# tunnel-group group1 type webvpn
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	設定一般モードを開始し、全般的なトンネル グループ属性を設定します。
tunnel-group ipsec-attributes	設定 ipsec モードを開始し、IPSec トンネル グループ属性を設定します。

コマンド	説明
tunnel-group ppp-attributes	L2TP 接続の PPP 設定を行うための設定 ppp モードを開始します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

tunnel-group general-attributes

一般属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、すべてのサポートされるトンネリング プロトコルに共通の設定値を設定するために使用されます。

すべての一般属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

構文の説明

general-attributes	このトンネル グループの属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	他のトンネル グループ タイプのさまざまな属性が、一般トンネル グループ属性リストに移行され、トンネル グループ一般属性モードのプロンプトが変更されました。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用してリモート アクセス接続のリモート アクセス トンネル グループを作成し、その後、トンネル グループ一般属性を設定するための一般属性コンフィギュレーション モードを開始する例を示します。トンネル グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type remote-access
hostname(config)# tunnel-group 209.165.200.225 general-attributes
hostname(config-tunnel-general)#
```

次に、グローバル コンフィギュレーション モードを開始し、IPSec リモート アクセス接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の一般属性を設定するための一般コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group ipsec-attributes

ipsec 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group ipsec-attributes** コマンドを使用します。このモードは、IPSec トンネリング プロトコルに固有の設定値を設定するために使用されます。

すべての IPSec 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

構文の説明

ipsec-attributes	このトンネル グループの属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	さまざまな IPSec トンネル グループ属性が一般トンネル グループ属性リストに移行され、トンネル グループ ipsec 属性モードのプロンプトが変更されました。

例

次に、グローバル コンフィギュレーション モードを開始し、IPSec リモート アクセス トンネル グループ remotegrp のトンネル グループを作成し、その後、IPSec グループ属性を指定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group ppp-attributes

ppp 属性コンフィギュレーション モードを開始し、IPSec を介した L2TP 接続によって使用される PPP 設定値を設定するには、グローバル コンフィギュレーション モードで **tunnel-group ppp-attributes** コマンドを使用します。

すべての PPP 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

構文の説明

name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PPP 設定値は Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）によって使用されます。L2TP は、リモート クライアントがダイヤルアップ電話サービスのパブリック IP ネットワークを使用してプライベート社内ネットワーク サーバとセキュアに通信できるようにする VPN トンネリング プロトコルです。L2TP はクライアント/サーバ モデルに基づき、PPP over UDP（ポート 1701）を使用してデータをトンネルします。tunnel-group ppp コマンドはすべて、PPPoE トンネル グループ タイプで使用できます。

例

次に、トンネル グループ *telecommuters* を作成し、ppp 属性コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# tunnel-group telecommuters type pppoe
hostname(config)# tunnel-group telecommuters ppp-attributes
hostname(tunnel-group-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group webvpn-attributes

webvpn 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードでは、WebVPN トンネリングに共通の設定値を設定します。

すべての WebVPN 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

構文の説明

webvpn-attributes	このトンネル グループの WebVPN 属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用して WebVPN 接続用のトンネル グループを作成し、その後、WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。トンネル グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type webvpn
hostname(config)# tunnel-group 209.165.200.225 webvpn-attributes
hostname(config-tunnel-webvpn)#
```

次に、グローバル コンフィギュレーション モードを開始し、WebVPN 接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# tunnel-group remotegrp type webvpn
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group-map default-group

tunnel-group-map default-group コマンドでは、他の設定された方式を使用して名前を判別できない場合に使用するデフォルトのトンネル グループを指定します。

tunnel-group-map を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

構文の説明

default-group *tunnel-group-name*	他の設定された方式では名前を取得できない場合に使用するデフォルトのトンネル グループを指定します。*tunnel-group name* はすでに存在している必要があります。
rule index	任意。**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map default-group のデフォルト値は DefaultRAGroup です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ ルールもこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は group1 です。

```
hostname(config)# tunnel-group-map default-group group1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	暗号 CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。

tunnel-group-map enable

tunnel-group-map enable コマンドでは、証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

構文の説明

policy	証明書からトンネル グループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。 **ike-id**：トンネル グループがルール ルックアップに基づいて判別されない、または ou から取得されない場合は、フェーズ 1 IKE ID の内容に基づいて証明書ベースの IKE セッションをトンネル グループにマッピングされることを示します。 **ou**：トンネル グループがルール ルックアップに基づいて判別されない場合は、サブジェクト Distinguished Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）の値が使用されることを示します。 **peer-ip**：トンネル グループが規則の検索に基づいて決定されないか、ou または ike-id メソッドから取得されない場合、確立されたピア IP アドレスを使用することを示します。 **rules**：このコマンドによって設定された証明書マップ アソシエーションに基づいて、証明書ベースの IKE セッションがトンネル グループにマッピングされることを示します。
rule index	任意。**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map コマンドのデフォルト値は **enable ou** で、**default-group** は DefaultRAGroup に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

例

次に、フェーズ 1 IKE ID の内容に基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次に、確立済みのピアの IP アドレスに基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次に、サブジェクト Distinguished Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）に基づく、証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次に、確立済みのルールに基づく証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルトのトンネル グループとして指定します。

tunnel-limit

セキュリティ アプライアンス上でアクティブになることが許可される GTP トンネルの最大数を指定するには、**gtp-map** コマンドを使用してアクセスする GTP マップ コンフィギュレーション モードで **tunnel limit** コマンドを使用します。トンネル制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

構文の説明

max_tunnels	トンネルの最大許容数です。グローバルなトンネル全体の制限の範囲は、1 ～ 4294967295 です。

デフォルト

トンネル制限のデフォルトは、500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。

例

次に、GTP トラフィックの最大トンネル数を 10,000 に指定する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

tx-ring-limit

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **tx-ring-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

構文の説明

number-of-packets	イーサネット送信ドライバが許容できる低遅延パケットまたは標準のプライオリティのパケットの最大数を指定します。このパケットの処理が終わると、イーサネット送信ドライバは輻輳が解消するまで、インターフェイス上のパケットをバッファしているキューの処理に戻ります。 **tx-ring-limit** の値の範囲は、PIX プラットフォームでは 3 から 128 パケットで、ASA プラットフォームでは 3 から 256 パケットです。

デフォルト

デフォルトの **tx-ring-limit** は、128 パケットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プライオリティ キュー	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、遅延の影響を受けやすい、プライオリティの高いトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）と、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）の 2 つのトラフィック クラスを使用できます。セキュリティ アプライアンスは、プライオリティ トラフィックを認識して、適切な Quality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にする前に、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューを作成する必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドで、プライオリティ キュー モードを開始します。これはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびパケットをドロップする前にバッファに入れることができる両タイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

（注）　インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する*必要があります*。

指定する tx-ring-limit および queue-limit は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの 2 つのパラメータを調整することで、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが、*テールドロップ*です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注）　**queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時にダイナミックに決定されます。この制限を表示するには、コマンド ラインに **help** または **?** と入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。**queue-limit** の値の範囲は、0 ～ 2048 パケットです。**tx-ring-limit** の値の範囲は、PIX プラットフォームでは 3 から 128 パケットで、ASA プラットフォームでは 3 から 256 パケットです。

ASA モデル 5505（のみ）では、1 つのインターフェイスにプライオリティ キューを設定すると、他のすべてのインターフェイスで同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけが、すべてのインターフェイスに存在することになります。さらに、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスからも削除されます。

この問題を回避するには、**priority-queue** コマンドを 1 つのインターフェイスにのみ設定します。**queue-limit** コマンドと **tx-ring-limit** コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次の例では、test というインターフェイスにプライオリティ キューを、キュー制限を 2048 パケットに、送信キュー制限を 256 パケットに設定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 2048
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。

コマンド	説明
show priority-queue statistics	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定した場合、このコマンドは、現在の **priority-queue**、**queue-limit**、および **tx-ring-limit** コマンドのコンフィギュレーション値をすべて表示します。

type echo

SLA 動作をエコー応答時間プローブ動作として設定するには、SLA モニタ コンフィギュレーション モードで **type echo** コマンドを使用します。SLA コンフィギュレーションからタイプを削除するには、このコマンドの **no** 形式を使用します。

type echo protocol ipIcmpEcho *target* interface *if-name*

no type echoprotocol ipIcmpEcho *target* interface *if-name*

構文の説明

interface *if-name*	エコー要求パケットを送信するために使用されるインターフェイスのインターフェイス名を、**nameif** コマンドで指定されているとおりに指定します。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。
protocol	プロトコルのキーワード。サポートされる唯一の値が **ipIcmpEcho** で、エコー動作で IP/ICMP エコー要求を使用するように指定します。
target	モニタするオブジェクトの IP アドレスまたはホスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ICMP パケットのペイロードのデフォルト サイズは 28 バイトで、合計サイズが 64 バイトの ICMP パケットを作成します。ペイロード サイズは、**request-data-size** コマンドを使用して変更できます。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。SLA の到達可能性を追跡するために、ID が 1 のトラッキング エントリを作成します。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	SLA 動作要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。

CHAPTER 33

undebug コマンド～ zonelabs integrity ssl-client-authentication コマンド

undebug

現在のセッションでデバッグ情報の表示をディセーブルにするには、特権 EXEC モードで **undebug** コマンドを使用します。

undebug {*command* | **all**}

構文の説明

command	指定したコマンドのデバッグをディセーブルにします。サポートされるコマンドの詳細については、「使用上のガイドライン」を参照してください。
all	すべてのデバッグ出力をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。このコマンドには、追加のデバッグ キーワードが含まれます。

使用上のガイドライン

次のコマンドは、undebug コマンドで使用できます。特定のコマンドのデバッグ、または特定の **debug** コマンドに関連付けられた引数とキーワードの詳細については、**debug** *command* のエントリを参照してください。

- aaa：AAA 情報
- acl：ACL 情報
- all：すべてのデバッグ
- appfw：アプリケーション ファイアウォール情報
- arp：NP オペレーションを含む ARP
- asdm：ASDM 情報
- auto-update：Auto-update 情報
- boot-mem：ブート メモリの計算と設定
- cifs：CIFS 情報
- cmgr：CMGR 情報
- context：コンテキスト情報
- cplane：CP 情報

- crypto：クリプト情報
- ctiqbe：CTIQBE 情報
- ctl-provider：CTL プロバイダーのデバッグ情報
- dap：DAP 情報
- dcerpc：DCERPC 情報
- ddns：ダイナミック DNS 情報
- dhcpc：DHCP クライアント情報
- dhcpd：DHCP サーバ情報
- dhcprelay：DHCP リレー情報
- disk：ディスク情報
- dns：DNS 情報
- eap：EAP 情報
- eigrp：EIGRP プロトコル情報
- email：電子メール情報
- entity：エンティティ MIB 情報
- eou：EAPoUDP 情報
- esmtp：ESMTP 情報
- fips：FIPS 140-2 情報
- fixup：フィックスアップ情報
- fover：フェールオーバー情報
- fsm：FSM 情報
- ftp：FTP 情報
- generic：その他の情報
- gtp：GTP 情報
- h323：H323 情報
- http：HTTP 情報
- icmp：ICMP 情報
- igmp：インターネット グループ管理プロトコル
- ils：LDAP 情報
- im：IM インスペクション情報
- imagemgr：Image Manager 情報
- inspect：デバッグ情報のインスペクション
- integrityfw：Integrity ファイアウォール情報
- ip：IP 情報
- ipsec-over-tcp：IPSec over TCP 情報
- IPSec-pass-thru：ipsec-pass-thru 情報のインスペクション
- ipv6：IPv6 情報
- iua-proxy：IUA プロキシ情報

- kerberos：KERBEROS 情報
- l2tp：L2TP 情報
- ldap：LDAP 情報
- mfib：マルチキャスト転送情報ベース
- mgcp：MGCP 情報
- module-boot：サービス モジュール ブート情報
- mrib：マルチキャスト ルーティング情報ベース
- nac-framework：NAC-FRAMEWORK 情報
- netbios-inspect：NETBIOS インスペクション情報
- npshim：NPSHIM 情報
- ntdomain：NT ドメイン情報
- ntp：NTP 情報
- ospf：OSPF 情報
- p2p：P2P インスペクション情報
- parser：パーサー情報
- pim：Protocol Independent Multicast
- pix：PIX 情報
- ppp：PPP 情報
- pppoe：PPPoE 情報
- pptp：PPTP 情報
- radius：RADIUS 情報
- redundant-interface：冗長インターフェイス情報
- rip：RIP 情報
- rtp：RTP 情報
- rtsp：RTSP 情報
- sdi：SDI 情報
- sequence：シーケンス番号の追加
- session-command：セッション コマンド情報
- sip：SIP 情報
- skinny：Skinny 情報
- sla：IP SLA モニタ デバッグ
- smtp-client：電子メール システムのログ メッセージ
- splitdns：スプリット DNS 情報
- sqlnet：SQLNET 情報
- ssh：SSH 情報
- sunrpc：SUNRPC 情報
- tacacs：TACACS 情報
- tcp：WebVPN の TCP

- tcp-map：TCP マップ情報
- timestamps：タイムスタンプの追加
- track：スタティック ルート トラッキング
- vlan-mapping：VLAN マッピング情報
- vpn-sessiondb：VPN セッション データベース情報
- vpnlb：VPN ロード バランシング情報
- wccp：WCCP 情報
- webvpn：WebVPN 情報
- xdmcp：XDMCP 情報
- xml：XML パーサー情報

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべてのデバッグ出力をディセーブルにする例を示します。

```
hostname(config)# undebug all
```

関連コマンド

コマンド	説明
debug	選択したコマンドに関するデバッグ情報を表示します。

unix-auth-gid

UNIX グループ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-gid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid <*identifier*>

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルト値は 65534 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

文字列で Network File System（NetFS; ネットワーク ファイル システム）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX グループ ID を 4567 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 4567
```

関連コマンド

コマンド	説明
unix-auth-uid	UNIX ユーザ ID を設定します。

unix-auth-uid

UNIX ユーザ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-uid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid <*identifier*>

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルト値は 65534 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

文字列で Network File System（NetFS; ネットワーク ファイル システム）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX ユーザ ID を 333 に設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 333
```

関連コマンド

コマンド	説明
unix-auth-gid	UNIX グループ ID を設定します。

upload-max-size

アップロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **upload-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

upload-max-size <*size*>

no upload-max-size

構文の説明

size	アップロードされるオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

サイズを 0 に設定すると、実質的にオブジェクトのアップロードは許可されません。

例

次に、アップロードされるオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# upload-max-size 1500
```

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
download-max-size	ダウンロードするオブジェクトの最大サイズを指定します。

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

urgent-flag

TCP ノーマライザを通して URG ポインタを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

構文の説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタをクリアします。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトでクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。その新しい TCP マップを、**policy-map** コマンドを使用して適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈を明確化していません。したがって、エンド システムにおいては緊急オフセットがさまざまな方法で処理されます。このため、エンド システムが攻撃を受けやすくなります。デフォルトの動作では、URG フラグとオフセットはクリアされます。

例

次に、緊急フラグを許可する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

uri-non-sip

Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別するには、パラメータ コンフィギュレーション モードで **uri-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

構文の説明

mask	SIP 以外の URI をマスクします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップの Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url

CRL を取得するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

構文の説明

index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。セキュリティ アプライアンスは、インデックス 1 から URL を試行します。
url	CRL の取得元となる URL を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL 設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

例

次に、ca-crl コンフィギュレーション モードを開始し、CRL 取得用の URL のリストを作成および維持するためにインデックス 3 を設定して CRL の取得元となる URL https://foobin.com を設定する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
policy	CRL の取得元を指定します。

url-block

フィルタリング サーバからのフィルタリング決定を待機する間、Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

構文の説明

block *block_buffer*	フィルタリング サーバからのフィルタリング決定を待機している間に Web サーバの応答を保存する HTTP 応答バッファを作成します。指定できる値は 1 ～ 128 です。これは、1550 バイトのブロック数を示します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズをキロバイト（KB）単位で設定します。指定できる値は 2 ～ 10240 です。これは、2 ～ 10240 KB の URL バッファ メモリ プールを示します。
url-size *long_url_size*	バッファに保存する長い各 URL の最大許容 URL サイズを KB 単位で設定します。最大 URL サイズとして指定できる値は、Websense では 2、3、または 4（それぞれ 2 KB、3 KB、4KB を表す）、Secure Computing では 2 または 3（それぞれ 2 KB、3 KB を表す）です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長い URL をフィルタリングできます。Secure Computing の場合は、**url-block url-size** コマンドを使用して、最大 3 KB の長い URL をフィルタリングできます。Websense フィルタリング サーバおよび N2H2

フィルタリング サーバの場合、**url-block block** コマンドを使用すると、セキュリティ アプライアンスは、URL フィルタリング サーバからの応答を待機している間、Web クライアント要求への応答として Web サーバから受信したパケットをバッファに保存します。これにより、Web クライアントのパフォーマンスがデフォルトのセキュリティ アプライアンス動作よりも向上します。デフォルトの動作では、パケットをドロップし、接続か許可された場合に Web サーバにパケットの再送信を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、セキュリティ アプライアンスはブロックを HTTP 応答バッファから Web クライアントに送信し、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、セキュリティ アプライアンスは拒否メッセージを Web クライアントに送信し、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答のバッファリングに使用するブロック数を指定します。

url-block url-size コマンドを **url-block mempool-size** コマンドとともに使用して、フィルタリングする URL の最大長と URL バッファに割り当てる最大メモリを指定します。Websense サーバまたは Secure-Computing サーバに、1159 バイトよりも長く、最大 4096 バイトまでの URL を渡す場合は、これらのコマンドを使用します。**url-block url-size** コマンドは、1159 バイトよりも長い URL をバッファに保存し、その URL を（TCP パケット ストリームを使用して）Websense サーバまたは Secure-Computing サーバに渡します。これにより、Websense サーバまたは Secure-Computing サーバでは、その URL へのアクセスを許可または拒否できます。

例

次に、URL フィルタリング サーバからの応答をバッファに保存するために 1550 バイトのブロックを 56 個割り当てる例を示します。

```
hostname#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-cache

Websense サーバから受信した URL 応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

構文の説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。このモードは、Websense サーバ上ですべてのユーザが同じ URL フィルタリング ポリシーを共有する場合に選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求の送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、Websense サーバ上でユーザが同じ URL フィルタリング ポリシーを共有しない場合に選択します。
statistics	**statistics** オプションを使用すると、キャッシュ ルックアップの回数やヒット率などの追加の URL キャッシュ統計情報が表示されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

（注）　N2H2 サーバ アプリケーションは、URL フィルタリングでこのコマンドをサポートしません。

url-cache コマンドには、URL サーバからの応答をキャッシュするコンフィギュレーション オプションが用意されています。

url-cache コマンドは、URL キャッシングのイネーブル化、キャッシュ サイズの設定、およびキャッシュ統計情報の表示を行う場合に使用します。

キャッシングにより、URL アクセス権限がセキュリティ アプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは要求を Websense サーバに転送するのではなく、一致するアクセス権限を URL キャッシュ内で探します。キャッシングをディセーブルにするには、**no url-cache** コマンドを使用します。

（注）　Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティ ニーズを満たす使用状況プロファイルを取得した後、**url-cache** をイネーブルにしてスループットを向上させます。Websense プロトコル バージョン 4 の URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、送信元アドレスと宛先アドレスに基づいてすべての発信 HTTP 接続をキャッシュする例を示します。

```
hostname(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-server	**filter** コマンドで使用する Websense サーバを指定します。

url-entry

ポータル ページで HTTP/HTTPS URL を入力する機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **url-entry** コマンドを使用します。

url-entry enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

例

次に、Finance という DAP レコードの URL エントリをイネーブルにする例を示します。

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# url-entry enable
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

url-length-limit

RTSP メッセージで許可される URL の最大長を設定するには、パラメータ コンフィギュレーション モードで **url-length-limit** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

url-length-limit *length*

no url-length-limit *length*

構文の説明

length	URL の長さ制限（バイト単位）。値の範囲は、0 ～ 6000 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、RTSP インスペクション ポリシー マップで URL の長さ制限を設定する例を示します。

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# url-length-limit 50
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url-list（削除）

このコマンドを使用して SSL VPN 接続によるアクセス用の URL リストを定義できなくなりました。今後は **import** コマンドを使用して、URL リストを定義する XML オブジェクトをインポートしてください。詳細については、**import-** コマンドと **export-url-list** コマンドを参照してください。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	このコマンドは廃止されました。このコマンドがソフトウェアのこのリリースに残されているのは、既存の URL リストの下位互換性を維持するためです。セキュリティ アプライアンスは、それらのリストを XML ファイルに変換できます。このコマンドを使用して新しい URL リストを作成することはできません。

使用上のガイドライン

グローバル コンフィギュレーション モードで url-list コマンドを使用して、1 つ以上の URL リストを作成します。特定のグループ ポリシーまたはユーザに対してリスト内の URL へのアクセスを許可するには、ここで作成した *listname* を、webvpn モードで **url-list** コマンドとともに使用します。

例

次に、www.cisco.com、www.example.com、および www.example.org へのアクセスを提供する *Marketing URLs* という名前の URL リストを作成する例を示します。次の表に、各 URL の設定で使用する値を示します。

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスは、そのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている URL のセットを表示します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

url-list（グループ ポリシー webvpn）

WebVPN サーバと URL のリストを特定のユーザまたはグループ ポリシーに適用するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを使用します。**url-list none** コマンドを使用して作成したヌル値を含むリストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストが継承されないようにするには、**url-list none** コマンドを使用します。次回このコマンドを使用すると、前回までの設定が上書きされます。

url-list {**value** *name* | **none**} [*index*]

no url-list

構文の説明

index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表に、このコマンドを入力するモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—
ユーザ名モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次回このコマンドを使用すると、前回までの設定が上書きされます。

webvpn モードで **url-list** コマンドを使用してユーザまたはグループ ポリシーの WebVPN ホームページに表示する URL リストを指定する前に、XML オブジェクトでリストを作成する必要があります。グローバル コンフィギュレーション モードで **import** コマンドを使用して、URL リストをセキュリティ アプライアンスにダウンロードします。次に、url-list コマンドを使用して、リストを特定のグループ ポリシーまたはユーザに適用します。

例

次に、FirstGroupURLs という名前の URL リストを FirstGroup という名前のグループ ポリシーに適用し、このリストを 1 番めの URL リストに指定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

関連コマンド

コマンド	説明
clear configure url-list [*listname*]	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスは、そのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている一連の **url-list** コマンドを表示します。
webvpn	webvpn モードを開始します。これは、webvpn コンフィギュレーション モード、グループ ポリシー webvpn コンフィギュレーション モード（特定のグループ ポリシーの webvpn 設定を行う場合）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザの webvpn 設定を行う場合）のいずれかです。

url-server

filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定するには、グローバル コンフィギュレーション モードで **url-server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

N2H2

url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

no url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

構文の説明

N2H2

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	（任意）認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
port *number*	N2H2 サーバ ポート。セキュリティ アプライアンスは、UDP 応答のリッスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、セキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。
vendor	「smartfilter」または「n2h2」（下位互換性を維持するため）を使用して URL フィルタリング サービスを指定します。ただし、「smartfilter」はベンダー ストリングとして保存されます。

Websense

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。

if_name	認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、セキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル バージョン 1 です。
vendor websense	URL フィルタリング サービスのベンダーが Websense であることを示します。
version	プロトコル バージョン **1** または **4** を指定します。デフォルトは TCP プロトコル バージョン 1 です。TCP は、バージョン 1 またはバージョン 4 を使用して設定できます。UDP は、バージョン 4 を使用してのみ設定できます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•		•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。URL サーバ数の上限は、シングル コンテキスト モードでは 16、マルチ コンテキスト モードでは 4 ですが、一度に使用できるアプリケーションは、N2H2 または Websense のいずれか 1 つのみです。さらに、セキュリティ アプライアンス上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションは更新されないため、ベンダーの指示に従って別途更新する必要があります。

HTTPS および FTP に対して **filter** コマンドを発行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連するすべての **filter** コマンドも削除されます。

サーバを指定した後、**filter url** コマンドを使用して URL フィルタリング サービスをイネーブルにします。

サーバの統計情報（到達不能サーバを含む）を表示するには、**show url-server statistics** コマンドを使用します。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の **url-server** コマンドの適切な形式を使用して、URL フィルタリング アプリケーション サーバを指定します。

ステップ 2　**filter** コマンドを使用して、URL フィルタリングをイネーブルにします。

ステップ 3　（任意）**url-cache** コマンドを使用して、URL キャッシングをイネーブルにし、認識される応答時間を短縮します。

ステップ 4　（任意）**url-block** コマンドを使用して、長い URL および HTTP バッファリングのサポートをイネーブルにします。

ステップ 5　**show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリング サービスの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次に、N2H2 の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、Websense の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。

user-authentication

ユーザ認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。実行コンフィギュレーションからユーザ認証属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。

user-authentication {**enable | disable**}

no user-authentication

構文の説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

個々のユーザは、設定した認証サーバの順序に従って認証されます。

プライマリ セキュリティ アプライアンスでユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーのユーザ認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルにすると、VPN クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
secure-unit-authentication	VPN クライアントに、トンネルを開始するたびにユーザ名とパスワードによる認証を要求することによって、セキュリティを強化します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間内にユーザ接続上で通信アクティビティが行われない場合、セキュリティ アプライアンスによって接続が切断されます。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。アイドル タイムアウト値が継承されないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間内にハードウェア クライアントの背後にいるユーザによって通信アクティビティが行われない場合、セキュリティ アプライアンスによって接続が切断されます。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

構文の説明

minutes	アイドル タイムアウト期間の分数を指定します。指定できる範囲は 1 ～ 35791394 分です。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトまたは指定したグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されないようにします。

デフォルト

30 分。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアント アクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して 45 分のアイドル タイムアウト値を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn モードで **user storage** コマンドを使用します。ユーザ ストレージをディセーブルにするには、このコマンドの **no** バージョンを使用します。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。

デフォルト

ユーザストレージはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、セキュリティ アプライアンスではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	
storage-objects	

username

ユーザをセキュリティ アプライアンス データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名を指定して、このコマンドの **no** 形式を使用します。すべてのユーザ名を削除するには、ユーザ名を指定せずに、このコマンドの **no** 形式を使用します。

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

no username *name*

構文の説明

encrypted	パスワードを暗号化することを示します（**mschap** を指定しなかった場合）。**username** コマンド内のパスワードを定義すると、セキュリティ アプライアンスはセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別のセキュリティ アプライアンスにカット アンド ペーストして、同じパスワードを使用する場合だけです。
mschap	パスワードを入力後に unicode に変換し、MD4 を使用してハッシュすることを指定します。このキーワードは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
name	ユーザの名前を 4 ～ 64 文字の長さのストリングとして指定します。
nopassword	このユーザにパスワードが必要ないことを示します。
nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 で使用するために暗号化することを示します。ユーザを追加するときに **mschap** キーワードを指定した場合は、**show running-config** コマンドを使用してコンフィギュレーションを表示すると、**encrypted** キーワードではなくこのキーワードが表示されます。 **username** コマンド内のパスワードを定義すると、セキュリティ アプライアンスはセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **nt-encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` CLI で実際に **nt-encrypted** キーワードを入力するのは、コンフィギュレーションを別のセキュリティ アプライアンスにカット アンド ペーストし、かつ、同じパスワードを使用する場合のみです。

password *password*	パスワードを 3 ～ 32 文字の長さのストリングとして指定します。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）の範囲で設定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンド認可で使用されます。

デフォルト

デフォルトの特権レベルは 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.2(1)	**mschap** キーワードと **nt-encrypted** キーワードが追加されました。

使用上のガイドライン

login コマンドでは、このデータベースを認証用に使用します。

CLI にアクセスできるユーザや特権モードを開始できないユーザをローカル データベースに追加する場合は、コマンド認可をイネーブルにする必要があります（**aaa authorization command** コマンドを参照）。コマンド認可をイネーブルにしなければ、ユーザは、特権レベルが 2 以上（デフォルトは 2）であれば、CLI で独自のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、AAA 認証を使用してユーザが **login** コマンドを使用できないようにするか、すべてのローカル ユーザをレベル 1 に設定して **enable** パスワードで特権 EXEC モードにアクセスできるユーザを制御できます。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。

例

次に、パスワードが 12345678、特権レベルが 12 の「anyuser」という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser password 12345678 privilege 12
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性コンフィギュレーション モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username-from-certificate

認可のためのユーザ名として、証明書内のいずれのフィールドを使用するかを指定するには、トンネルグループ一般属性モードで **username-from-certificate** コマンドを使用します。認可のためのユーザ名として使用するピア証明書の DN

属性をコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

構文の説明

primary-attr	証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
secondary-attr	（任意）デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
use-entire-name	セキュリティ アプライアンスでは、完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。

デフォルト

プライマリ属性のデフォルト値は CN（一般名）です。

セカンダリ属性のデフォルト値は OU（組織の部門）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ユーザ名として使用する証明書内のフィールドを選択します。このコマンドは、リリース 8.0.4 以降で廃止された **authorization-dn-attributes** コマンドに代わるものです。**username-from-certificate** コマンドは、セキュリティ アプライアンスに、指定した証明書フィールドをユーザ名 / パスワード認可のためのユーザ名として使用するように強制します。

ユーザ名 / パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたこのユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドも設定する必要があります。つまり、ユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）: 2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）: 個人、システムなどの名前。セカンダリ属性としては使用できません。
DNQ	Domain Name Qualifier（ドメイン名修飾子）。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）: 組織が置かれている市または町。
N	名前
O	Organization（組織）: 会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）: Organization（O; 組織）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）: 組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、プライマリ属性として CN（一般名）、セカンダリ属性として OU を使用して、デジタル証明書から認可クエリーの名前を取得するように指定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

username attributes

ユーザ名属性モードを開始するには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザの属性をすべて削除するには、このコマンドの **no** 形式を使用し、ユーザ名を付加します。すべてのユーザの属性をすべて削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。属性モードを使用すると、指定したユーザに対して属性値ペアを設定できます。

username {*name*} **attributes**

no username [*name*] **attributes**

構文の説明

name	ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	**service-type** 属性が追加されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザ名属性は、**username** コマンドまたは **username attributes** コマンドを使用して設定できます。

設定ユーザ名コンフィギュレーション モードのコマンドの構文には、次のような共通する特徴があります。

- **no** 形式を使用すると、実行コンフィギュレーションから属性が削除されます。
- **none** キーワードを使用しても、実行コンフィギュレーションから属性が削除されます。ただし、このキーワードでは、属性をヌル値に設定し、継承されないようにすることによって、このことを行います。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

username attributes コマンドは、設定ユーザ名モードを開始し、次の属性を設定できるようにします。

属性	機能
group-lock	ユーザが接続する必要がある既存のトンネル グループを指定します。
password-storage	クライアント システムでのログイン パスワードの保存をイネーブルまたはディセーブルにします。
service-type [login | framed | vpn | admin | nas-prompt]	コンソール ログインを制限し、適切なレベルが割り当てられているユーザのログインをイネーブルにします。**login** オプションでは、基本的な AAA サービスを指定します。これはデフォルトです。**framed** オプションも、基本的な AAA サービスを指定します。**vpn** オプションでは、リモート アクセスのための基本的な AAA サービスを指定します。**admin** オプションは、AAA サービス、ログイン コンソール特権、EXEC モード特権、イネーブル特権、および CLI 特権を指定します。**nas-prompt** オプションは、AAA サービス、ログイン コンソール特権、および EXEC モード特権を指定しますが、イネーブル特権は指定しません。
vpn-access-hours	設定済みの時間範囲ポリシーの名前を指定します。
vpn-filter	ユーザ固有の ACL の名前を指定します。
vpn-framed-ip-address	クライアントに割り当てる IP アドレスとネット マスクを指定します。
vpn-group-policy	属性の継承元となるグループ ポリシーの名前を指定します。
vpn-idle-timeout	アイドル タイムアウト期間を分単位で指定するか、または **none** を指定してディセーブルにします。
vpn-session-timeout	最大ユーザ接続時間を分単位で指定するか、または **none** を指定して時間を無制限にします。
vpn-simultaneous-logins	許可される同時ログインの最大数を指定します。
vpn-tunnel-protocol	使用できるトンネリング プロトコルを指定します。
webvpn	webvpn モードを開始して、webvpn 属性を設定できるようにします。

ユーザ名の webvpn モード属性を設定するには、ユーザ名 webvpn コンフィギュレーション モードで **username attributes** コマンドを入力してから、**webvpn** コマンドを入力します。詳細については、**webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）の説明を参照してください。

例

次に、「anyuser」という名前のユーザのユーザ名属性コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。

コマンド	説明
username	セキュリティ アプライアンス データベースにユーザを追加します。
webvpn	ユーザ名 webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

username-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのユーザ名プロンプトをカスタマイズするには、Webvpn カスタマイゼーション モードで **username-prompt** コマンドを使用します。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

ユーザ名プロンプトのデフォルト テキストは、「USERNAME:」です。

ユーザ名プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、テキストを「Corporate Username:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# username-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。

user-alert

現在のアクティブ セッションのすべてのクライアントレス SSL VPN ユーザに対して、緊急メッセージをブロードキャストするには、特権 EXEC モードで **user-alert** コマンドを使用します。メッセージをディセーブルにするには、このコマンドの no user-alert 形式を使用します。

user-alert *string cancel*

no user-alert

構文の説明

cancel	ポップアップ ブラウザ ウィンドウの起動を取り消します。
string	英数字

デフォルト

値のデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、設定されたメッセージを含むポップアップ ブラウザ ウィンドウがエンドユーザに表示されます。このコマンドでは、セキュリティ アプライアンス コンフィギュレーション ファイルは変更されません。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
hostname # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
hostname #
```

user-message

DAP レコードが選択されたときに表示するテキスト メッセージを指定するには、ダイナミック アクセス ポリシー レコード モードで user-message コマンドを使用します。このメッセージを削除するには、このコマンドの **no** 形式を使用します。同じ DAP レコードに対してコマンドを複数回使用した場合、前のメッセージは新しいメッセージに置き換えられます。

user-message *message*

no user-message

構文の説明

message	この DAP レコードに割り当てられているユーザに対するメッセージ。最大 128 文字を入力できます。メッセージにスペースを含める場合は、メッセージを二重引用符で囲みます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

SSL VPN 接続に成功すると、ポータル ページに、クリック可能な点滅するアイコンが表示されます。ユーザはそのアイコンをクリックして、接続に関連付けられているメッセージを確認できます。DAP ポリシーからの接続が終了し（アクション = 終了）、その DAP レコードにユーザ メッセージが設定されている場合は、そのメッセージがログイン画面に表示されます。

複数の DAP レコードが接続に適用される場合、セキュリティ アプライアンスは該当するユーザ メッセージを組み合わせて 1 つのストリングとして表示します。

例

次に、Finance という DAP レコードに「Hello Money Managers」というユーザ メッセージを設定する例を示します。

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# user-message "Hello Money Managers"
hostname(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

user-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **user-parameter** を使用します。これは HTTP フォームのコマンドを使用した SSO です。

user-parameter *name*

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	HTTP POST 要求に含まれているユーザ名パラメータの名前。名前の最大の長さは 128 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。要求されたコマンド **user-parameter** は、HTTP POST 要求に SSO 認証用のユーザ名パラメータを含める必要があることを指定します。

（注）　ログイン時に、ユーザは実際の名前を入力します。この名前は、HTTP POST 要求に入力されて認証 Web サーバに渡されます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、SSO 認証に使用される HTTP POST 要求にユーザ名パラメータ userid を含めることを指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn モードで **user storage** コマンドを使用します。ユーザ ストレージをディセーブルにするには、このコマンドの **no** バージョンを使用します。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。

デフォルト

ユーザストレージはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、セキュリティ アプライアンスではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	
storage-objects	

validate-attribute

RADIUS アカウンティングの使用時に RADIUS 属性を検証するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **validate attribute** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

このオプションは、デフォルトで無効です。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

構文の説明

attribute_number	RADIUS アカウンティングで検証する RADIUS 属性。値の範囲は、1 ～ 191 です。ベンダー固有属性はサポートされません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
radius アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定すると、セキュリティ アプライアンスは、Framed IP 属性に加えて RADIUS 属性に対する照合も実行します。このコマンドは、インスタンスを複数設定できます。

RADIUS 属性タイプのリストは、インターネット割り当て番号局の Web サイトで参照できます。

http://www.iana.org/assignments/radius-types/radius-types.xml

例

次に、ユーザ名 RADIUS 属性の RADIUS アカウンティングをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# validate attribute 1
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

validation-policy（クリプト CA トラスト ポイント）

着信ユーザ接続に関連付けられている証明書を検証するためにトラストポイントを使用できる条件を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-policy** コマンドを使用します。指定した条件でトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[no] validation-policy {ssl | ipsec} [no-chain] [subordinate-only]

構文の説明

ipsec	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを IPSec 接続の検証に使用できることを指定します。
no-chain	セキュリティ デバイス上にない下位証明書のチェーンをディセーブルにします。
ssl	トラストポイントと関連付けられている Certificate Authority（CA; 認証局）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。
subordinate-only	このトラストポイントで表される CA から直接発行されたクライアント証明書の検証をディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド履歴

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

リモート アクセス VPN では、配置の要件に応じて、Secure Sockets Layer（SSL）VPN、IP Security（IPSec; IP セキュリティ）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。**validation-policy** コマンドを使用して、オンボード CA 証明書へのアクセスに使用できるプロトコル タイプを指定できます。

このコマンドで **no-chain** オプションを指定すると、セキュリティ アプライアンスは、そのセキュリティ アプライアンスでトラストポイントとして設定されていない下位 CA 証明書をサポートできません。

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。これにより、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能がイネーブルになっている別のトラストポイントにすでに関連付けられている CA に対して認証

される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# validation-policy ssl
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントが指定したトラストポイントの下位証明書を受け入れるように設定する例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# validation-policy subordinates-only
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

verify

ファイルのチェックサムを確認するには、特権 EXEC モードで **verify** コマンドを使用します。

verify *path*

verify /md5 *path* [*md5-value*]

構文の説明

/md5	（任意）指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
md5-value	（任意）指定したイメージの既知の MD5 値。コマンドで MD5 値を指定すると、指定したイメージの MD5 値が計算され、MD5 値が一致するかどうかを示すメッセージが表示されます。
path	• **disk0:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:**/[*path*/]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用可能であり、外部フラッシュ メモリ カードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、**flash** は **disk0** のエイリアスです。 • **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**：ASCII 受動モード – **an**：ASCII 通常モード – **ip**：（デフォルト）バイナリ受動モード – **in**：バイナリ通常モード • **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**verify** コマンドではなく **tftp-server** コマンドでパスを設定します。

デフォルト

現在のフラッシュ デバイスがデフォルトのファイル システムです。

（注）　**/md5** オプションを指定する場合、ftp、http、tftp などのネットワーク ファイルをソースとして使用できます。**/md5** オプションを指定せずに **verify** コマンドを使用した場合は、フラッシュのローカル イメージのみを確認できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

verify コマンドを使用して、ファイルを使用する前にそのチェックサムを確認します。

ディスクで配布される各ソフトウェア イメージでは、イメージ全体に対して 1 つのチェックサムが使用されます。このチェックサムは、イメージをフラッシュ メモリにコピーする場合にのみ表示され、イメージ ファイルをあるディスクから別のディスクにコピーする場合は表示されません。

新しいイメージをロードまたは複製する前に、そのイメージのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリまたはサーバにコピーするときにチェックサムを確認できるようにします。Cisco.com では、さまざまなイメージ情報を入手できます。

フラッシュ メモリの内容を表示するには、**show flash** コマンドを使用します。フラッシュ メモリの内容のリストには、個々のファイルのチェックサムは含まれません。イメージをフラッシュ メモリにコピーした後で、そのイメージのチェックサムを再計算して確認するには、**verify** コマンドを使用します。ただし、**verify** コマンドでは、ファイルがファイル システムに保存された後にのみ、整合性チェックを実行します。破損しているイメージがセキュリティ アプライアンスに転送され、検出されずにファイル システムに保存される場合があります。破損しているイメージが正常にセキュリティ アプライアンスに転送されると、ソフトウェアはイメージが壊れていることを把握できず、ファイルの確認が正常に完了します。

Message-Digest5（MD5; メッセージ ダイジェスト 5）ハッシュ アルゴリズムを使用してファイルを検証するには、**/md5** オプションを指定して **verify** コマンドを使用します。MD5（RFC 1321 で規定）は、一意の 128 ビットのメッセージ ダイジェストを作成することによってデータ整合性を確認するアルゴリズムです。**verify** コマンドの **/md5** オプションを使用すると、セキュリティ アプライアンスのソフトウェア イメージの MD5 チェックサム値を、その既知の MD5 チェックサム値と比較することによって、イメージの整合性を確認できます。すべてのセキュリティ アプライアンスのソフトウェア イメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。

MD5 整合性チェックを実行するには、**/md5** キーワードを指定して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェア イメージの MD5 値が計算され、表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、まず Cisco.com から MD5 値を取得し、その値をコマンド構文で指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しない場合は、いずれかのイメージが破損しているか、または入力した MD5 値が正しくありません。

例

次に、cdisk.bin というイメージ ファイルに対して使用された verify コマンドの例を示します。わかりやすくするために、一部のテキストは省略されています。

```
hostname# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
hostname#
```

関連コマンド

コマンド	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

version

セキュリティ アプライアンスでグローバルに使用する RIP のバージョンを指定するには、ルータ コンフィギュレーション モードで **version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {**1** | **2**}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは、バージョン 1 およびバージョン 2 のパケットを受信しますが、送信するのはバージョン 1 のパケットのみです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを入力することによって、インターフェイスごとにグローバルな設定を上書きすることができます。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、すべてのインターフェイスで RIP バージョン 2 のパケットを送受信するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

構文の説明

ip_address	セキュリティ アプライアンス上の仮想 HTTP サーバの IP アドレスを設定します。このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。
warning	（任意）HTTP 接続をセキュリティ アプライアンスにリダイレクトする必要があることをユーザに通知します。このキーワードは、リダイレクトが自動的に行われないテキストベースのブラウザにのみ適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	以前のリリースで使用されていたインライン基本 HTTP 認証方式がリダイレクション方式に置き換えられたため、このコマンドは廃止され、不要になりました。
7.2(2)	**aaa authentication listener** コマンドを使用して、基本 HTTP 認証（デフォルト）と HTTP リダイレクションのいずれを使用するかを選択できるようになったため、このコマンドは復活しました。リダイレクション方式では、HTTP 認証をカスケードするための特別なコマンドは必要ありません。

使用上のガイドライン

セキュリティ アプライアンスで HTTP 認証を使用する場合は（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、セキュリティ アプライアンスで基本 HTTP 認証がデフォルトで使用されます。**redirect** キーワードを指定した **aaa authentication listener** を使用して、セキュリティ アプライアンスが HTTP 接続をセキュリティ アプライアンスによって生成された Web ページにリダイレクトするように認証方式を変更できます。

ただし、基本 HTTP 認証の使用を続行する場合は、HTTP 認証をカスケードするときに **virtual http** コマンドが必要になることがあります。

セキュリティ アプライアンスに加えて宛先 HTTP サーバで認証が必要な場合は、**virtual http** コマンドを使用して、セキュリティ アプライアンス（AAA サーバ経由）と HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

このコマンドは、AAA 認証を必要とするすべての HTTP 接続をセキュリティ アプライアンス上の仮想 HTTP サーバにリダイレクトします。セキュリティ アプライアンスにより、AAA サーバのユーザ名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバがユーザを認証すると、セキュリティ アプライアンスは HTTP 接続を元のサーバにリダイレクトして戻しますが、AAA サーバのユーザ名とパスワードは含めません。HTTP パケットにユーザ名とパスワードが含まれていないため、HTTP サーバによりユーザに HTTP サーバのユーザ名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 HTTP アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 HTTP IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

（注）　**virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの期間を 0 秒に設定しないでください。設定すると、実際の Web サーバへの HTTP 接続ができなくなります。

例

次に、AAA 認証とともに仮想 HTTP をイネーブルにする例を示します。

```
hostname(config)# virtual http 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list ACL-IN remark This is the HTTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list ACL-IN remark This is the virtual HTTP address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list AUTH remark This is the HTTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list AUTH remark This is the virtual HTTP address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
aaa authentication listener http	セキュリティ アプライアンスが認証に使用する方式を設定します。
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。

sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにする場合は、このコマンドを使用すると、ブラウザ キャッシュ内のユーザ名とパスワードを使用して仮想サーバに再接続できます。
virtual telnet	セキュリティ アプライアンス上に仮想 Telnet サーバを設定して、認証を必要とする他のタイプの接続を開始する前に、ユーザをセキュリティ アプライアンスで認証できるようにします。

virtual telnet

セキュリティ アプライアンス上に仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。セキュリティ アプライアンスによって認証プロンプトが表示されない他のタイプのトラフィックに対する認証が必要な場合は、仮想 Telnet サーバでユーザを認証する必要があります。サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

virtual telnet *ip_address*

no virtual telnet *ip_address*

構文の説明

ip_address	セキュリティ アプライアンス上の仮想 Telnet サーバの IP アドレスを設定します。このアドレスは必ず、セキュリティ アプライアンスにルーティングされる未使用のアドレスにしてください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

任意のプロトコルまたはサービスのネットワーク アクセス認証を設定できますが（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、HTTP、Telnet、または FTP のみで直接認証することもできます。ユーザはまずこれらのサービスのいずれかで認証を行ってから、認証を要求する他のトラフィックの通過を認可する必要があります。HTTP、Telnet、または FTP のセキュリティ アプライアンスの通過を許可せず、その他のタイプのトラフィックを認証する場合は、セキュリティ アプライアンス上で設定された所定の IP アドレスにユーザが Telnet で接続し、セキュリティ アプライアンスによって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

authentication match コマンドまたは **aaa authentication include** コマンドを使用して、仮想 Telnet アドレスおよび認証するその他のサービスへの Telnet アクセスに対する認証を設定する必要があります。

認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを求められ、その後 AAA サーバにより認証されます。認証されると、ユーザには「Authentication Successful.」というメッセージが表示されます。それ以降、ユーザは認証を必要とする他のサービスに正常にアクセスできます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 Telnet アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 Telnet IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

セキュリティ アプライアンスからログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

例

次に、他のサービスに対する AAA 認証とともに仮想 Telnet をイネーブルにする例を示します。

```
hostname(config)# virtual telnet 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
hostname(config)# access-list ACL-IN remark This is the virtual Telnet address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
hostname(config)# access-list AUTH remark This is the virtual Telnet address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求する場合は、このコマンドを使用して、セキュリティ アプライアンスと HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

vlan

VLAN ID をサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスでは、トラフィックを通過させるために VLAN ID が必要です。VLAN サブインターフェイスを使用して、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLAN を使用すると、所定の物理インターフェイス上で複数のセキュリティ コンテキストなどのトラフィックを別々に保管できます。

vlan *id*

no vlan

構文の説明

id	1 ～ 4094 の範囲の整数を指定します。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

1 つの VLAN をサブインターフェイスにのみ割り当てることができます。物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、セキュリティ アプライアンスによって古い ID が変更されます。

サブインターフェイスをイネーブルにするには、**no shutdown** コマンドを使用して物理インターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。したがって、インターフェイスの停止によってトラフィックが物理インターフェイスを通過しないようにすることはできません。代わりに、**nameif** コマンドを省略することによって、トラフィックが物理インターフェイスを通過しないようにします。物理インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって異なります。プラットフォームごとのサブインターフェイスの最大数については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

例

次に、VLAN 101 をサブインターフェイスに割り当てる例を示します。

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、VLAN を 102 に変更する例を示します。

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vlan（グループ ポリシー）

VLAN をグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで **vlan** コマンドを使用します。グループ ポリシーのコンフィギュレーションから VLAN を削除し、デフォルトのグループ ポリシーの VLAN 設定に置き換えるには、このコマンドの **no** 形式を使用します。

[**no**] **vlan** {*vlan_id* |**none**}

構文の説明

vlan_id	このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）。インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用して、このセキュリティ アプライアンスに VLAN を設定する必要があります。
none	このグループ ポリシーに一致するリモート アクセス VPN セッションへの VLAN の割り当てをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。

デフォルト

デフォルト値は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.3(0)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、このグループ ポリシーに割り当てられているセッションの出力 VLAN インターフェイスを指定します。セキュリティ アプライアンスは、このグループのすべてのトラフィックを指定された VLAN に転送します。VLAN を各グループ ポリシーに割り当ててアクセス コントロールを簡素化できます。このコマンドは、セッション上のトラフィックをフィルタリングする ACL の代わりに使用します。

例

次のコマンドでは、VLAN 1 をグループ ポリシーに割り当てます。

```
hostname(config-group-policy)# vlan 1
hostname(config-group-policy)
```

次のコマンドでは、VLAN マッピングをグループ ポリシーから削除します。

```
hostname(config-group-policy)# vlan none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
`show vlan`	セキュリティ アプライアンスに設定されている VLAN を表示します。
`vlan`（インターフェイス コンフィギュレーション モード）	サブインターフェイスに VLAN ID を割り当てます。
`show vpn-session_summary.db`	IPSec、Cisco AnyConnect、NAC の各セッションの数および使用中の VLAN の数を表示します。
`show vpn-session.db`	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

vpdn group

VPDN グループを作成または編集し、PPPoE クライアントを設定するには、グローバル コンフィギュレーション モードで **vpdn group** コマンドを使用します。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

vpdn group *group_name* {**localname** *username* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** *name* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

vpdn group *group_name*	VPDN グループの名前を指定します。
localname *username*	ユーザ名を認証のために VPDN グループにリンクし、**vpdn username** コマンドで設定された名前と照合する必要があります。
request dialout pppoe	ダイヤルアウト PPPoE 要求を許可することを指定します。
ppp authentication {chap | mschap | pap}}	Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）認証プロトコルを指定します。Windows クライアントのダイヤルアップ ネットワーク設定を使用して、使用する認証プロトコル（PAP、CHAP、または MS-CHAP）を指定できます。クライアントで指定した設定は、セキュリティ アプライアンスで使用する設定と一致している必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）を使用すると、PPP ピアは相互に認証できます。PAP は、ホスト名またはユーザ名をクリアテキストで渡します。Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）を使用すると、PPP ピアは、アクセス サーバとの通信によって不正アクセスを防止できます。MS-CHAP は Microsoft 版の CHAP です。PIX Firewall では、MS-CHAP バージョン 1 のみサポートされます（バージョン 2.0 はサポートされません）。 ホストで認証プロトコルが指定されていない場合は、コンフィギュレーションで **ppp authentication** オプションを指定しないでください。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.1	このコマンドが導入されました。

使用上のガイドライン　Virtual Private Network（VPDN; バーチャル プライベート ネットワーク）は、リモート ダイヤルイン ユーザとプライベート ネットワーク間の長距離のポイントツーポイント接続を提供するために使用します。セキュリティ アプライアンス上の VDPN では、レイヤ 2 トンネリング技術の PPPoE を使用して、リモート ユーザからパブリック ネットワーク経由のプライベート ネットワークへのダイヤルアップ ネットワーク接続を確立します。

PPPoE は、Point-to-Point Protocol（PPP）over Ethernet です。PPP は、IP、IPX、ARA などのネットワーク層プロトコルで動作するように設計されています。PPP には、セキュリティ メカニズムとして CHAP と PAP も組み込まれています。

PPPoE 接続のセッション情報を表示するには、**show vpdn session pppoe** コマンドを使用します。コンフィギュレーションからすべての **vpdn group** コマンドを削除して、すべてのアクティブな L2TP トンネルと PPPoE トンネルを停止するには、**clear configure vpdn group** コマンドを使用します。**clear configure vpdn username** コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

PPPoE は PPP をカプセル化するため、PPPoE は PPP を使用して、認証および VPN トンネル内で動作しているクライアント セッションに対する ECP 機能と CCP 機能を実行します。さらに、PPP によって PPPoE に IP アドレスが割り当てられるため、PPPoE と DHCP の併用はサポートされません。

（注）　PPPoE に VPDN グループが設定されていない場合、PPPoE は接続を確立できません。

PPPoE に使用する VPDN グループを定義するには、**vpdn group** *group_name* **request dialout pppoe** コマンドを使用します。次に、インターフェイス コンフィギュレーション モードで **pppoe client vpdn group** コマンドを使用して、VPDN グループを特定のインターフェイス上の PPPoE クライアントに関連付けます。

ISP が認証を要求している場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドを使用して、ISP で使用される認証プロトコルを選択します。

ISP によって割り当てられたユーザ名を VPDN グループに関連付けるには、**vpdn group** *group_name* **localname** *username* コマンドを使用します。

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、**vpdn username** *username* password *password* コマンドを使用します。ユーザ名は、PPPoE に指定した VPDN グループにすでに関連付けられているユーザ名にする必要があります。

（注）　ISP で CHAP または MS-CHAP が使用されている場合、ユーザ名はリモート システム名、パスワードは CHAP シークレットと呼ばれることがあります。

PPPoE クライアント機能はデフォルトでオフになっているため、VPDN の設定後、**ip address** *if_name* **pppoe** [**setroute**] コマンドを使用して PPPoE をイネーブルにします。**setroute** オプションを指定すると、デフォルト ルートが存在しない場合にデフォルト ルートが作成されます。

PPPoE の設定後すぐに、セキュリティ アプライアンスは通信する PPPoE アクセス コンセントレータを探します。PPPoE 接続が正常終了または異常終了すると、セキュリティ アプライアンスは通信する新しいアクセス コンセントレータを探します。

次の **ip address** コマンドは、PPPoE セッションの開始後に使用しないでください。使用すると、PPPoE セッションが終了します。

- **ip address outside pppoe**：このコマンドは新しい PPPoE セッションを開始しようとします。
- **ip address outside dhcp**：このコマンドは、インターフェイスがその DHCP 設定を取得するまでインターフェイスをディセーブルにします。
- **ip address outside** *address netmask*：インターフェイスが正常に初期化されたインターフェイスとして起動するため。

例

次に、VDPN グループ *telecommuters* を作成し、PPPoE クライアントを設定する例を示します。

```
F1(config)# vpdn group telecommuters request dialout pppoe
F1(config)# vpdn group telecommuters localname user1
F1(config)# vpdn group telecommuters ppp authentication pap
F1(config)# vpdn username user1 password test1
F1(config)# interface GigabitEthernet 0/1
F1(config-subif)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group *group_name*	VPDN グループのコンフィギュレーションを表示します。
vpdn username	PPPoE 接続用のユーザ名とパスワードのペアを作成します。

vpdn username

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、グローバル コンフィギュレーション モードで **vpdn username** コマンドを使用します。

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

username	ユーザ名を指定します。
password	パスワードを指定します。
store-local	ユーザ名とパスワードをセキュリティ アプライアンス上の NVRAM の特別な場所に保存します。Auto Update Server が clear config コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

VPDN ユーザ名は、**vpdn group** *group_name* **localname** *username* コマンドで指定された VPDN グループにすでに関連付けられているユーザ名にする必要があります。

clear configure vpdn username コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

例

次に、パスワードが *telecommuter*9/8 の *bob_smith* という VPDN ユーザ名を作成する例を示します。

```
F1(config)# vpdn username bob_smith password telecommuter9/8
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group	VPDN グループのコンフィギュレーションを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

vpn-access-hours

グループ ポリシーを設定済み time-range ポリシーに関連付けるには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値が継承されないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

構文の説明

none	VPN アクセス時間をヌル値に設定して、time-range ポリシーを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

デフォルト

制限なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup というグループ ポリシーを 824 という time-range ポリシーに関連付ける例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日と 1 日の時間を設定します（開始日と終了日を含む）。

vpn-addr-assign

IP アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。設定したすべての VPN アドレス割り当て方法をセキュリティ アプライアンスから削除するには、このコマンドの **no** 形式を使用します。引数なしで

vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

構文の説明

aaa	外部または内部（ローカル）AAA 認証サーバから IP アドレスを取得します。
dhcp	DHCP 経由で IP アドレスを取得します。
local	セキュリティ アプライアンスに設定されている IP アドレス プールから IP アドレスを割り当てて、トンネル グループに関連付けます。
reuse-delay *delay*	解放された IP アドレスを再利用するまでの遅延時間。指定できる範囲は 0 ～ 480 分です。デフォルトは 0（ディセーブル）です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(3)	**reuse-delay** オプションが追加されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバが使用できる IP アドレスの範囲も定義する必要があります。DHCP サーバが使用する IP アドレスを指定するには、**dhcp-server** コマンドを使用する必要があります。

ローカルを選択する場合は、**ip local pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。次に、**vpn-framed-ip-address** コマンドと **vpn-framed-netmask** コマンドを使用して、IP アドレスとネットマスクを個々のユーザに割り当てます。

ローカル プールを使用する場合は、**reuse-delay** *delay* オプションを使用して、解放された IP アドレスを再利用するまでの遅延時間を調整します。遅延時間を長くすると、IP アドレスがプールに戻されて即座に再割り当てされるときにファイアウォールで発生する可能性がある問題を回避できます。

AAA を選択する場合は、設定済みのいずれかの RADIUS サーバから IP アドレスを取得します。

例

次に、アドレス割り当て方法として DHCP を設定する例を示します。

```
hostname(config)# vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	セキュリティ アプライアンス DHCP サーバがグループ ポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲を指定します。
ip local pool	ローカル IP アドレス プールを作成します。
vpn-framed-ip-address	特定のユーザに割り当てる IP アドレスを指定します。
vpn-framed-ip-netmask	特定のユーザに割り当てるネットマスクを指定します。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グローバル ポリシーまたはユーザ名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含む ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値が継承されないようにするには、**vpn-filter none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACL name*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

vpn-filter コマンドで定義された ACL は、クライアントレス SSL VPN 接続には適用されません。この ACL は、IPSec と SSL VPN クライアント セッションのみに適用されます。

例

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。

vpn-framed-ip-address

特定のユーザに割り当てる IP アドレスを指定するには、ユーザ名モードで **vpn-framed-ip-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

構文の説明

ip_address	このユーザの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

vpn-group-policy

ユーザが設定済みのグループ ポリシーから属性を継承するようにするには、ユーザ名コンフィギュレーション モードで **vpn-group-policy** コマンドを使用します。グループ ポリシーをユーザ コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、ユーザはユーザ名レベルで設定されていない属性を継承できます。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

構文の説明

group-policy name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定ユーザのグループ ポリシーの属性値を上書きするには、その値をユーザ名モードで設定します（その属性をユーザ名モードで使用できる場合）。

例

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザを設定する例を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーをセキュリティ アプライアンス データベースに追加します。
group-policy attributes	グループ ポリシー属性モードを開始します。これにより、グループ ポリシーの AVP を設定できます。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	ユーザ名属性モードを開始します。これにより、特定のユーザの AVP を設定できます。

vpn-idle-timeout

ユーザ タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがない場合、セキュリティ アプライアンスは接続を終了します。

実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout {*minutes* | **none**}

no vpn-idle-timeout

構文の説明

minutes	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

30 分。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して 15 分の VPN アイドル タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続の最大許容時間を設定します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

vpn load-balancing

VPN ロード バランシングおよび関連機能を設定できる VPN ロード バランシング モードを開始するには、グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを使用します。

vpn load-balancing

（注）　VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	ASA Model 5510（Plus ライセンス付き）および ASA Model 5520 以降のサポートが追加されました。

使用上のガイドライン

ロード バランシング クラスタには、セキュリティ アプライアンス モデル 5510（Plus ライセンス付き）または ASA 5520 以降を含めることができます。VPN 3000 シリーズのコンセントレータも含めることができます。混合コンフィギュレーションは可能ですが、通常は、同種クラスタにする方が容易に管理できます。

vpn load-balancing コマンドを使用して、VPN ロード バランシング モードを開始します。VPN ロード バランシング モードでは、次のコマンドを使用できます。

- cluster encryption
- cluster ip address
- cluster key

- cluster port
- interface
- nat
- participate
- priority
- redirect-fqdn

詳細については、個々のコマンドの説明を参照してください。

例

次に、**vpn load-balancing** コマンドの例を示します。プロンプトが変わる点に注意してください。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

次に、interface コマンドを含む VPN load-balancing コマンド シーケンスの例を示します。interface コマンドでは、クラスタのパブリック インターフェイスを「test」、クラスタのプライベート インターフェイスを「foo」と指定しています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。

vpn-sessiondb logoff

すべての VPN セッションまたは選択した VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**remote** | **l2l** | **webvpn** | **email-proxy** | **protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all**}

構文の説明

all	すべての VPN セッションをログオフします。
email-proxy	すべての電子メール プロキシ セッションをログオフします。
index *indexnumber*	インデックス番号で 1 つのセッションをログオフします。セッションのインデックス番号を指定します。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザ名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルは次のとおりです。 IKE　POP3S IMAP4S　SMTPS IPSec　userHTTPS IPSecLAN2LAN　vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	すべてのリモートアクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループのセッションをログオフします。
webvpn	すべての WebVPN セッションをログオフします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべてのリモートアクセス セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff remote
```

次に、すべての IPSec セッションをログオフする例を示します。

hostname# **vpn-sessiondb logoff protocol IPSec**

vpn-sessiondb max-session-limit

VPN セッションをセキュリティ アプライアンスで許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-session-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-session-limit {*session-limit*}

no **vpn-sessiondb max-session-limit**

構文の説明

session-limit	許可される最大 VPN セッション数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IPSec VPN セッションに適用されます。

例

次に、最大 VPN セッション数の制限を 450 に設定する例を示します。

```
hostname# vpn-sessiondb max-session-limit 450
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび WebVPN セッションをログオフします。
vpn-sessiondb max-webvpn-session-limit	WebVPN セッションの最大数を設定します。

vpn-sessiondb max-webvpn-session-limit

SSL VPN セッションをセキュリティ アプライアンスで許可されているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-webvpn-session-limit** コマンドを使用します。セッションの制限を削除するには、このコマンドの **no** バージョンを使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-webvpn-session-limit {*session-limit*}

no vpn-sessiondb max-webvpn-session-limit

構文の説明

session-limit	許可される最大 WebVPN セッション数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SSL VPN セッション（AnyConnect VPN Client、レガシー SSL VPN Client（SVC）、クライアントレス（以前の WebVPN）セッションなど）に適用されます。

例

次に、最大セッション数の制限を 75 に設定する例を示します。

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび SSL VPN セッションをログオフします。
vpn-sessiondb max-vpn-session-limit	VPN セッションの最大数を設定します。

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout {*minutes* | **none**}

no vpn-session-timeout

構文の説明

minutes	タイムアウト期間の分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許可します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがない場合、セキュリティ アプライアンスは接続を終了します。

vpn-simultaneous-logins

ユーザに許可される同時ログイン数を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

構文の説明

integer	0 ～ 2147483647 の数字。

デフォルト

デフォルトの同時ログイン数は、3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

（注） 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPSec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

例

次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネル タイプ（IPSec、L2TP over IPSec、SVC、または WebVPN）を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

no vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

構文の説明

IPSec	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
l2tp-ipsec	L2TP 接続の IPSec トンネルをネゴシエートします。
svc	SSL VPN クライアントについて SSL VPN トンネルをネゴシエートします。
webvpn	HTTPS 対応の Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは必要ありません。

デフォルト

デフォルトは IPSec です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グループ ポリシー コンフィギュレーション	•	—	•	—	—
ユーザ名コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**l2tp-ipsec** キーワードが追加されました。
7.3(1)	**svc** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

（注） IPSec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** 引数と **ipsec** 引数の両方を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して WebVPN トンネリング モードと IPSec トンネリング モードを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

関連コマンド

コマンド	説明
address pools	アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

vpnclient connect

設定済みサーバへの Easy VPN Remote 接続の確立を試行するには、グローバル コンフィギュレーション モードで **vpnclient connect** コマンドを使用します。

vpnclient connect

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

例

次に、設定済み EasyVPN サーバへの Easy VPN リモート接続の確立を試行する例を示します。

```
hostname(config)# vpnclient connect
hostname(config)#
```

vpnclient disconnect

Easy VPN Remote 接続を切断するには、グローバル コンフィギュレーション モードで **vpnclient disconnect** コマンドを使用します。

vpnclient disconnect

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

例

次に、Easy VPN Remote 接続を切断する例を示します。

```
hostname(config)# vpnclient disconnect
hostname(config)#
```

vpnclient enable

Easy VPN Remote 機能をイネーブルにするには、グローバル コンフィギュレーション モードで **vpnclient enable** コマンドを使用します。Easy VPN Remote 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

vpnclient enable

no vpnclient enable

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA 5505 にのみ適用されます。

vpnclient enable コマンドを入力すると、ASA 5505 は Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれます）として機能します。

例

次に、Easy VPN Remote 機能をイネーブルにする例を示します。

```
hostname(config)# vpnclient enable
hostname(config)#
```

次に、Easy VPN Remote 機能をディセーブルにする例を示します。

```
hostname(config)# no vpnclient enable
hostname(config)#
```

vpnclient ipsec-over-tcp

Easy VPN ハードウェア クライアントとして動作している ASA 5505 を、TCP カプセル化 IPSec を使用するように設定するには、グローバル コンフィギュレーション モードで **vpnclient ipsec-over-tcp** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

構文の説明

port	（任意）特定のポートを使用するように指定します。
tcp_port	（**port** キーワードを指定する場合は必須）TCP カプセル化 IPSec トンネルに使用する TCP ポート番号を指定します。

デフォルト

コマンドでポート番号を指定しない場合、Easy VPN Remote 接続では、ポート 10000 が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 にのみ適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバは、IPSec をユーザ データグラム プロトコル（UDP）パケットにカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準の Encapsulating Security Protocol（ESP; カプセル化セキュリティ プロトコル、プロトコル 50）または Internet Key Exchange（IKE; インターネット キー交換、UDP 500）を使用するには、TCP パケット内に IPSec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。ただし、UDP が許可されている環境では、IPSec over TCP を設定すると不要なオーバーヘッドが発生します。

TCP カプセル化 IPSec を使用するように ASA 5505 を設定する場合は、次のコマンドを入力して、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

このコマンドは、Don't Fragment（DF）ビットをカプセル化されたヘッダーからクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

例

次に、デフォルト ポート 10000 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

次に、ポート 10501 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

vpnclient mac-exempt

Easy VPN Remote 接続の背後にあるデバイスに対して個々のユーザ認証要件を免除するには、グローバル コンフィギュレーション モードで **vpnclient mac-exempt** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

構文の説明

mac_addr_1	ドット付き 16 進表記の MAC アドレス。個々のユーザ認証を免除するデバイスの製造業者とシリアル番号を指定します。デバイスが複数の場合は、スペースで区切った各 MAC アドレスとそれぞれのネットワーク マスクを指定します。 MAC アドレスの最初の 6 文字はデバイスの製造業者を識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。
mac_mask_1	対応する MAC アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の MAC アドレスとネットワーク マスクのペアを区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

Cisco IP Phone、無線アクセス ポイント、プリンタなどのデバイスは、認証を実行できないため、個々のユニット認証がイネーブルになっている場合でも認証されません。個々のユーザ認証がイネーブルになっている場合は、このコマンドを使用してこれらのデバイスの認証を免除できます。デバイスに対する個々のユーザ認証の免除は、「デバイス パススルー」とも呼ばれます。

このコマンドでは、MAC アドレスとマスクは、3 つの 16 進数をピリオドで区切って指定します。たとえば、MAC マスク ffff.ffff.ffff は、指定した MAC アドレスとのみ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスとも一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。

例

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

次に、1 つの特定の Cisco IP Phone を免除する例を示します。このようにすると、セキュリティは向上しますが、柔軟性が低くなります。

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

vpnclient management

Easy VPN ハードウェア クライアントへの管理アクセス用の IPSec トンネルを生成するには、グローバル コンフィギュレーション モードで **vpnclient management** コマンドを使用します。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。これにより、管理専用の IPSec トンネルが **split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って設定されます。

no vpnclient management

構文の説明

clear	通常のルーティングを使用して、社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセスを提供します。このオプションでは、管理トンネルは作成されません。 **（注）** このオプションは、クライアントとインターネット間で NAT デバイスが動作している場合に使用します。
ip_addr	Easy VPN ハードウェア クライアントからの管理トンネルを構築するホストまたはネットワークの IP アドレス。この引数は、**tunnel** キーワードとともに使用します。スペースで区切った 1 つ以上の IP アドレスとそれぞれのネットワーク マスクを指定します。
ip_mask	対応する IP アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の IP アドレスとネットワーク マスクのペアを区切ります。
tunnel	社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセス専用 IPSec トンネルを自動的に設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。ASA 5505 のコンフィギュレーションに次のコマンドが含まれていることを前提とします。

vpnclient server：ピアを指定します。

vpnclient mode：クライアント モード（PAT）またはネットワーク拡張モードを指定します。

次のいずれかが必要です。

- **vpnclient vpngroup**：Easy VPN サーバで認証に使用するトンネル グループと IKE 事前共有キーを指定します。
- **vpnclient trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを指定します。

vpnclient enable：ASA 5505 を Easy VPN クライアントとしてイネーブルにします。

（注） NAT デバイスでスタティック NAT マッピングを追加しなければ、NAT デバイスの背後にある ASA 5505 のパブリック アドレスにはアクセスできません。

例

次に、ASA 5505 の外部インターフェイスから IP アドレスとマスクの組み合わせが 192.168.10.10 255.255.255.0 であるホストへの IPSec トンネルを生成する例を示します。

```
hostname(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
hostname(config)#
```

次に、IPSec を使用しないで ASA 5505 の外部インターフェイスへの管理アクセスを提供する例を示します。

```
hostname(config)# vpnclient management clear
hostname(config)#
```

vpnclient mode

クライアント モードまたはネットワーク拡張モードの Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient mode** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

構文の説明

client-mode	クライアント モード（PAT）を使用するように Easy VPN Remote 接続を設定します。
network-extension-mode	ネットワーク拡張モード（NEM）を使用するように Easy VPN Remote 接続を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。Easy VPN クライアントは、クライアント モードまたは NEM のいずれかの動作モードをサポートします。動作モードによって、企業ネットワークからトンネル経由で内部ホスト（Easy VPN クライアントから見た場合の内部ホスト）に接続できるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

- クライアント モードでは、Easy VPN クライアントは、内部ホストからのすべての VPN トラフィックに対してポート アドレス変換（PAT）を実行します。このモードでは、ハードウェア クライアント（デフォルトの RFC 1918 アドレスが割り当てられています）の内部アドレスまたは内部ホストに対する IP アドレス管理は必要ありません。PAT により、企業ネットワークから内部ホストにはアクセスできません。

- NEM では、内部ネットワーク上のすべてのノードおよび内部インターフェイスに企業ネットワークでルーティング可能なアドレスが割り当てられます。内部ホストには、企業ネットワークからトンネル経由でアクセスできます。内部ネットワーク上のホストには、アクセス可能なサブネットから IP アドレスが（スタティックに、または DHCP によって）割り当てられます。ネットワーク拡張モードの場合、PAT は VPN トラフィックに適用されません。

（注）　Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続している場合は、各ヘッドエンド デバイスで **crypto map set reverse-route** コマンドを使用して、Reverse Route Injection（RRI; 逆ルート注入）によるリモート ネットワークのダイナミック通知を設定します。

例

次に、クライアント モードの Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient mode client-mode
hostname(config)#
```

次に、NEM の Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient mode network-extension-mode
hostname(config)#
```

vpnclient nem-st-autoconnect

NEM およびスプリット トンネリングが設定されている場合に、IPSec データ トンネルを自動的に開始するように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient nem-st-autoconnect** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。

vpnclient nem-st-autoconnect コマンドを入力する前に、ハードウェア クライアントのネットワーク拡張モードがイネーブルになっていることを確認します。ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要があります。トンネルのアップ後、いずれの側からでもデータ交換を開始できます。

（注） ネットワーク拡張モードをイネーブルにするように Easy VPN サーバを設定する必要もあります。そのためには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。

ネットワーク拡張モードでは、スプリット トンネリングが設定されている場合を除き、IPSec データ トンネルが自動的に開始し、保持されます。

例

次に、スプリット トンネリングが設定されたネットワーク拡張モードで自動的に接続するように Easy VPN Remote 接続を設定する例を示します。グループ ポリシー FirstGroup のネットワーク拡張モードがイネーブルになっています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

関連コマンド

コマンド	説明
nem	ハードウェア クライアントのネットワーク拡張モードをイネーブルにします。

vpnclient server-certificate

証明書マップによって指定された特定の証明書を持つ Easy VPN サーバへの接続のみを受け入れるように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient server-certificate** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

構文の説明

certmap_name	受け入れ可能な Easy VPN サーバ証明書を指定する証明書マップの名前を指定します。最大長は、64 文字です。

デフォルト

Easy VPN サーバ証明書のフィルタリングは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

このコマンドを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップ自体は、crypto ca certificate map コマンドと crypto ca certificate chain コマンドを使用して定義します。

例

次に、homeservers という名前の証明書マップを持つ Easy VPN サーバへの接続のみをサポートするように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient server-certificate homeservers
hostname(config)#
```

関連コマンド

コマンド	説明
certificate	指定された証明書を追加します。
vpnclient trustpoint	Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定します。

vpnclient server

Easy VPN Remote 接続用のプライマリおよびセカンダリ IPSec サーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient server *ip_primary_address* [*ip_secondary_address_1 ... ipsecondary_address_10*]

no vpnclient server

構文の説明

ip_primary_address	プライマリ Easy VPN（IPSec）サーバの IP アドレスまたは DNS 名。ASA または VPN 3000 コンセントレータ シリーズは、Easy VPN サーバとして機能できます。
ip_secondary_address_n	（任意）最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

接続を確立する前にサーバを設定する必要があります。**vpnclient server** コマンドでは、IPv4 アドレス、名前データベース、または DNS 名がサポートされ、アドレスはその順に解決されます。

サーバの IP アドレスまたはホスト名を使用できます。

例

次に、名前 headend-1 をアドレス 10.10.10.10 に関連付け、**vpnclient server** コマンドを使用して 3 台のサーバ（headend-dns.domain.com（プライマリ）、headend-1（セカンダリ）、および 192.168.10.10（セカンダリ））を指定する例を示します。

```
hostname(config)# names
hostname(config)# 10.10.10.10 headend-1
hostname(config)# vpnclient server headend-dns.domain.com headend-1 192.168.10.10
hostname(config)#
```

次に、VPN クライアントに IP アドレスが 10.10.10.15 のプライマリ IPSec サーバおよび IP アドレスが 10.10.10.30 と 192.168.10.45 のセカンダリ サーバを設定する例を示します。

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
hostname(config)#
```

vpnclient trustpoint

Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定するには、グローバル コンフィギュレーション モードで **vpnclient trustpoint** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

構文の説明

chain	証明書チェーン全体を送信します。
trustpoint_name	認証に使用する RSA 証明書を識別するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 にのみ適用され、また、デジタル証明書を使用する場合にのみ適用されます。

crypto ca trustpoint コマンドを使用してトラストポイントを定義します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

例

次に、central という名前の特定のアイデンティティ証明書を使用し、証明書チェーン全体を送信するように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードを開始し、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続の VPN ユーザ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient username** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

構文の説明

xauth_password	XAUTH に使用するパスワードを指定します。最大長は、64 文字です。
xauth_username	XAUTH に使用するユーザ名を指定します。最大長は、64 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは ASA モデル 5505 にだけ適用されます。

XAUTH ユーザ名とパスワードのパラメータは、セキュア ユニット認証がディセーブルで、サーバが XAUTH クレデンシャルを要求する場合に使用します。セキュア ユニット認証がイネーブルの場合、これらのパラメータは無視され、セキュリティ アプライアンスによって、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。

例

次に、XAUTH ユーザ名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する例を示します。

```
hostname(config)# vpnclient username testuser password ppurkm1
hostname(config)#
```

vpnclient vpngroup

Easy VPN Remote 接続の VPN トンネル グループ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient vpngroup** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

構文の説明

group_name	Easy VPN サーバで設定された VPN トンネル グループの名前を指定します。最大の長さは 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバで認証に使用する IKE 事前共有キー。最大長は 128 文字です。

デフォルト

Easy VPN クライアントとして動作している ASA 5505 のコンフィギュレーションでトンネル グループが指定されていない場合、クライアントは RSA 証明書を使用しようとします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれます）として動作している ASA 5505 に対してのみ適用されます。

事前共有キーをパスワードとして使用します。接続の確立前にサーバを設定する必要があります。

例

次に、グループ名が TestGroup1、パスワードが my_key123 の VPN トンネル グループを Easy VPN Remote 接続に設定する例を示します。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

関連コマンド

コマンド	説明
vpnclient trustpoint	Easy VPN 接続で使用する RSA アイデンティティ証明書を設定します。

wccp

容量を割り当て、サービス グループに参加できるように、指定した Web Cache Communication Protocol（WCCP）サービスのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **wccp** コマンドを使用します。サービス グループをディセーブルにし、容量の割り当てを解除するには、このコマンドの no 形式を使用します。

wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password]

no wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password [**0** | **7**]]

構文の説明

web-cache	Web キャッシュ サービスを指定します。 **（注）** Web キャッシュは、1 つのサービスとしてカウントされます。サービスの最大数（service-number 引数で割り当てられたサービスを含む）は 256 です。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。
redirect-list	（任意）このデバイス グループにリダイレクトされたトラフィックを制御するアクセス リストとともに使用します。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。アクセス リストには、ネットワーク アドレスだけを含める必要があります。ポート固有のエントリはサポートされていません。
access-list	アクセス リストの名前を指定します。
group-list	（任意）サービス グループへの参加を許可する Web キャッシュを決定するアクセス リスト。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
password	（任意）サービス グループから受信したメッセージに対して Message Digest 5（MD5）認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。
password	認証で使用するパスワードを指定します。password 引数の長さは最大 7 文字です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、サービス グループに参加できるように WCCP をイネーブルにする例を示します。

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

wccp redirect

Web Cache Communication Protocol（WCCP）を使用したインターフェイスの入口でのパケット リダイレクションをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP リダイレクションをディセーブルにするには、このコマンドの no 形式を使用します。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

構文の説明

interface_name	パケットをリダイレクトするインターフェイスの名前。
service	サービス グループを指定します。**web-cache** キーワードを指定するか、サービスの識別番号（0 ～ 99）を指定できます。
in	パケットがこのインターフェイスに着信するときにリダイレクションを実行するように指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、Web キャッシュ サービスの内部インターフェイスでの WCCP リダイレクションをイネーブルにする例を示します。

```
hostname(config)# wccp interface inside web-cache redirect in
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。

web-agent-url

セキュリティ アプライアンスが SiteMinder-type SSO 認証を要求する SSO サーバの URL を指定するには、config-webvpn-sso-siteminder モードで **web-agent-url** コマンドを使用します。

SSO サーバの認証 URL を削除するには、このコマンドの **no** 形式を使用します。

web-agent-url *url*

no web-agent-url *url*

（注） このコマンドは、SiteMinder-type SSO 認証に必要です。

構文の説明

url	SiteMinder-type SSO サーバの認証 URL を指定します。http:// または https:// を含める必要があります。

デフォルト

デフォルトでは、認証 URL は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
config-webvpn-sso-siteminder	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、さまざまなサーバで各種のセキュアなサービスにアクセスできます。SSO サーバには、認証要求を処理する URL があります。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

この URL に認証を送信するようにセキュリティ アプライアンスを設定するには、**web-agent-url** コマンドを使用します。認証 URL を設定する前に、**sso-server** コマンドを使用して SSO サーバを作成する必要があります。

セキュリティ アプライアンスと SSO サーバ間で https 通信を行うには、SSL 暗号化設定が両側で一致することを確認します。セキュリティ アプライアンスでは、これを **ssl encryption** コマンドで確認します。

例

次に、config-webvpn-sso-siteminder モードで認証 URL として http://www.example.com/webvpn を指定する例を示します。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
ssl encryption	SSL/TLS プロトコルで使用される暗号化アルゴリズムを指定します。
sso-server	シングル サインオン サーバを作成します。

web-applications

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Application] ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **web-applications** コマンドを使用します。

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「Web Application」です。

デフォルトのタイトルのスタイルは background-color:#99CCCC;color:black;font-weight:bold;text-transform uppercase です。uppercase です。

デフォルトのメッセージのテキストは「Enter Web Address (URL)」です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:maroon;font-size:smaller です。

デフォルトのドロップダウンのテキストは「Web Bookmarks」です。

デフォルトのドロップダウンのスタイルは border:1px solid black;font-weight:bold;color:black;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Applications」に変更し、テキストの色を青に変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-applications title text Applications
F1-asa1(config-webvpn-custom)# web-applications title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

web-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズするには、webvpn カスタマイゼーション モードで **web-bookmarks** コマンドを使用します。

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「Web Bookmarks」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Web Bookmarks] のタイトルを「Corporate Web Bookmarks」にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。

webvpn

webvpn モードを開始するには、グローバル コンフィギュレーション モードで **webvpn** コマンドを入力します。このコマンドで入力したコマンドを削除するには、**no webvpn** コマンドを使用します。これらの webvpn コマンドは、すべての WebVPN ユーザに適用されます。

これらの webvpn コマンドを使用して、AAA サーバ、デフォルト グループ ポリシー、デフォルト アイドル タイムアウト、http プロキシと https プロキシ、WebVPN 用の NBNS サーバ、およびエンド ユーザに表示される WebVPN 画面の外観を設定できます。

webvpn

no webvpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この WebVPN モードでは、WebVPN のグローバル設定を指定できます。グローバル ポリシー モードまたはユーザ名モードから WebVPN モードを開始した場合は、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

例

次に、WebVPN コマンド モードを開始する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)#
```

webvpn（グループ ポリシーおよびユーザ名モード）

この webvpn モードを開始するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用します。webvpn モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

グループ ポリシーおよびユーザ名に対する webvpn コマンドでは、ファイルへのアクセス、MAPI プロキシ、URL、および WebVPN を介した TCP アプリケーションを定義できます。ACL およびフィルタリングするトラフィックのタイプも指定します。

webvpn

no webvpn

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードから webvpn モードを開始した場合は、WebVPN のグローバル設定を指定できます。グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用すると、webvpn コマンドで指定された設定が親コマンドで指定されたグループまたはユーザに適用されます。つまり、ここで説明したグローバル ポリシー モードまたはユーザ名モードから開始した webvpn モードでは、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループ ポリシー属性モードで特定のグループ ポリシーに対して適用した WebVPN 属性は、デフォルト グループ ポリシーで指定された WebVPN 属性を上書きします。ユーザ名属性モードで特定のユーザに対して適用した WebVPN 属性は、デフォルト グループ ポリシー内およびそのユーザが属しているグループ ポリシー内の WebVPN 属性を上書きします。基本的に、これらのコマンドを使用すると、デフォルト グループまたは指定したグループ ポリシーから継承される設定を調整できます。WebVPN 設定の詳細については、グローバル コンフィギュレーション モードの **webvpn** コマンドに関する説明を参照してください。

次の表に、webvpn グループ ポリシー属性モードおよびユーザ名属性モードで設定できる属性を示します。詳細については、個々のコマンドの説明を参照してください。

属性	説明
auto-signon	WebVPN ユーザのログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定して、WebVPN ユーザにシングル サインオン方式を提供します。
customization	適用する設定済み WebVPN カスタマイゼーションを指定します。
deny-message	アクセスが拒否されたときにユーザに表示されるメッセージを指定します。
filter	WebVPN 接続に使用するアクセス リストを指定します。
functions	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を介した URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示される Web ページの URL を設定します。
html-content-filter	WebVPN セッションでフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
http-comp	使用する HTTP 圧縮アルゴリズムを指定します。
keep-alive-ignore	セッションの更新で無視する最大オブジェクト サイズを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに対する TCP ポート フォワーディングを識別する表示名を設定します。
sso-server	SSO サーバ名を設定します。
svc	SSL VPN クライアント属性を設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバと URL のリストを指定します。

例

次に、「FirstGroup」という名前のグループ ポリシーの webvpn モードを開始する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-webvpn)#
```

次に、「test」というユーザ名の webvpn モードを開始する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

関連コマンド

clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。

show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

who

セキュリティ アプライアンス上のアクティブな Telnet 管理セッションを表示するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

構文の説明

local_ip	（任意）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

who コマンドを使用すると、現在セキュリティ アプライアンスにログインしている各 Telnet クライアントの TTY_ID と IP アドレスを表示できます。

例

次に、クライアントが Telnet セッションを使用してセキュリティ アプライアンスにログインしている場合の **who** コマンドの出力例を示します。

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	セキュリティ アプライアンス コンソールへの Telnet アクセスを追加して、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

構文の説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続の許可です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用して、ウィンドウ サイズが縮小されたすべての接続をドロップします。

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

例

次に、さまざまなウィンドウ サイズの接続をすべてドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
```

```
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーから WINS サーバを継承できます。サーバが継承されないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

構文の説明

none	WINS サーバをヌル値に設定して、WINS サーバを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。複数のサーバを設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーに IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の WINS サーバを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定します。コンテキスト コンフィギュレーションを削除する場合は、ファイルをリモート サーバ（指定されている場合）から手動で削除するか、またはシステム実行スペースで **delete** コマンドを使用してファイルをフラッシュ メモリからクリアできます。

例

次に、スタートアップ コンフィギュレーションを消去する例を示します。

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write memory

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory [**all** [**/noconfirm**]]

構文の説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトを表示しません。
all	マルチ コンテキスト モードのシステム実行スペースでこのキーワードを使用すると、すべてのコンテキスト コンフィギュレーションおよびシステム コンフィギュレーションが保存されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	**all** キーワードを使用して、すべてのコンテキスト コンフィギュレーションを保存できるようになりました。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。変更内容は、起動時に実行メモリにロードされるスタートアップ コンフィギュレーションに保存した場合、次のリブートまでの間のみ保持されます。シングル コンテキスト モードまたはマルチ コンテキスト モードにおけるシステムのスタートアップ コンフィギュレーションの場所は、**boot config** コマンドを使用して、デフォルトの場所（隠しファイル）から選択した場所に変更できます。マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定された場所にあります。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力して、現在のコンテキスト コンフィギュレーションを保存できます。すべてのコンテキスト コンフィギュレーションを保存するには、システム実行スペースで **write memory all** コマンドを入力します。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、セキュリティ アプライアンスは、コンフィギュレーションをサーバに戻して保存できない HTTP および HTTPS の URL を除き、**config-url** コマンドで指定されたサーバにコンフィギュレーションを戻して保存します。セキュリティ アプライアンスが **write memory all** コマンドを使用して各コンテキストを保存した後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- フラッシュ メモリに不良セクターがあるためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

システムでは、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるため、**write memory** コマンドでも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次に、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する例を示します。

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。

コマンド	説明
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

実行コンフィギュレーションを TFTP サーバに保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 ファイル名をこのコマンドと **tftp-server** コマンドで指定した場合、セキュリティ アプライアンスは **tftp-server** コマンドのファイル名をディレクトリとして処理し、**write net** コマンドのファイル名をそのディレクトリの下にファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバでこのタイプの URL がサポートされていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。 デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。

マルチ コンテキスト モードの場合、このコマンドは現在のコンフィギュレーションを保存します。1 つのコマンドですべてのコンテキストを保存することはできません。このコマンドを、システムおよび各コンテキストに対して個別に入力する必要があります。**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、**write memory** コマンドでは、管理コンテキスト インターフェイスを使用してスタートアップ コンフィギュレーションに保存します。これは、システムで、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるからです。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次に、**tftp-server** コマンドで TFTP サーバおよびファイル名を設定する例を示します。

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドは入力されていません。

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドでディレクトリ名が設定され、サーバ アドレスは上書きされます。

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置にセキュリティ アプライアンスまたはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、コンフィギュレーションのスタンバイ ユニットまたはスタンバイ フェールオーバー グループと、アクティブなユニットまたはフェールオーバー グループのコンフィギュレーションとの同期が失われた場合にのみ、使用します。通常、この状態は、コマンドがスタンバイ ユニットまたはスタンバイ フェールオーバー グループで入力された場合に発生します。

Active/Standby フェールオーバーの場合、**write standby** コマンドはアクティブなフェールオーバー ユニットの RAM に保存されているコンフィギュレーションをスタンバイ ユニットの RAM に書き込みます。プライマリ ユニットとセカンダリ ユニットのコンフィギュレーションに含まれている情報が異なる場合に、**write standby** コマンドを使用します。このコマンドは、アクティブなユニットで入力します。

アクティブ/アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力した場合は、セキュリティ アプライアンス上のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストのコンフィギュレーションがピア ユニットに書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。
- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

（注）　**write standby** コマンドは、コンフィギュレーションをピア ユニットの実行コンフィギュレーションに複製します。コンフィギュレーションは、スタートアップ コンフィギュレーションに保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したユニットで **copy running-config startup-config** コマンドを使用します。コマンドはピア ユニットに複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

ステートフル フェールオーバーがイネーブルの場合、**write standby** コマンドは、コンフィギュレーションのレプリケーションが完了した後、状態情報もスタンバイ ユニットに複製します。

例

次に、現在の実行コンフィギュレーションをスタンバイ ユニットに書き込む例を示します。

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ ユニットを強制的にリブートします。

write terminal

端末で実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次に、実行コンフィギュレーションを端末に書き込む例を示します。

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

zonelabs-integrity fail-close

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生したときに VPN クライアントへの接続が閉じるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-close** コマンドを使用します。Zone Labs 接続で障害が発生しても VPN 接続を開いたままにするデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、接続は障害が発生しても開いたままです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合も、セキュリティ アプライアンスはプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。

Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生してもセキュリティ アプライアンスによってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバが応答しない場合、または接続が中断された場合に、VPN クライアント接続を閉じるようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity fail-close
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity fail-open

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生した後も、セキュリティ アプライアンスへのリモート VPN クライアント接続を開いたままにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-open** コマンドを使用します。Zone Labs サーバ接続で障害が発生した場合に VPN クライアントへの接続を閉じるには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスで Zone Labs Integrity ファイアウォール サーバへの接続が確立または維持されない場合、リモート VPN 接続は開いたままになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合も、セキュリティ アプライアンスはプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生してもセキュリティ アプライアンスによってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドまたは **no zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても VPN クライアント接続を開いたままにするデフォルト状態に戻す例を示します。

```
hostname(config)# zonelabs-integrity fail-open
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。

zonelabs-integrity fail-timeout

セキュリティ アプライアンスにおいて、何秒経過すると応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすかを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-timeout** コマンドを使用します。デフォルトのタイムアウト（10 秒）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

構文の説明

timeout	セキュリティ アプライアンスにおいて、応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすまでの秒数。設定可能な値の範囲は、5 ～ 20 秒です。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが指定された秒数待機しても Zone Labs サーバから応答がない場合、サーバは応答不能と見なされます。VPN クライアントへの接続は、デフォルトまたは **zonelabs-integrity fail-open** コマンドの設定に従って開いたままになります。ただし、**zonelabs-integrity fail-close** コマンドが発行されている場合は、セキュリティ アプライアンスで Integrity サーバが応答不能と見なされると接続は閉じます。

例

次に、12 秒経過後にアクティブな Zone Labs Intergity サーバを到達不能と見なすようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity fail-timeout 12
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity interface

Zone Labs Integrity サーバとの通信で使用するセキュリティ アプライアンス インターフェイスを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity interface** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのインターフェイスをデフォルト（none）にリセットするには、このコマンドの **no** 形式を使用します。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

構文の説明

interface	Zone Labs Integrity ファイアウォール サーバが通信するセキュリティ アプライアンス インターフェイスを指定します。これは、多くの場合、**nameif** コマンドで作成されたインターフェイス名です。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール インターフェイスは none に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、IP アドレス範囲 10.0.0.5 ～ 10.0.0.7 を使用して 3 台の Zone Labs Intergity サーバを設定する例を示します。また、これらのコマンドでは、ポート 300 および inside というインターフェイスでサーバをリッスンするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
hostname(config)# zonelabs-integrity port 300
hostname(config)# zonelabs-integrity interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

コマンド	説明
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity port

Zone Labs Integrity ファイアウォール サーバとの通信で使用するセキュリティ アプライアンス上のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity port** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのデフォルト ポート 5054 に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

構文の説明

port	セキュリティ アプライアンス上の Zone Labs Integrity ファイアウォール サーバのポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバのポートの番号。指定できる範囲は、10 ～ 10000 です。

デフォルト

Zone Labs Integrity ファイアウォール サーバのデフォルト ポートは 5054 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、**zonelabs-integrity port** コマンドと **zonelabs-integrity interface** コマンドでそれぞれ設定されたポートとインターフェイスで Zone Labs Integrity ファイアウォール サーバをリッスンします。

（注） 現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 を使用して Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、デフォルト ポート 5054 ではなくポート 300 でアクティブな Zone Labs サーバをリッスンするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
```

```
hostname(config)# zonelabs-integrity port 300
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity server-address

Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンス コンフィギュレーションに追加するには、グローバル コンフィギュレーション モードで **zonelabs-integrity server-address** コマンドを使用します。Zone Labs サーバを IP アドレスまたはホスト名で指定します。

Zone Labs Integrity ファイアウォール サーバを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

（注） ユーザ インターフェイスは複数の Integrity サーバのコンフィギュレーションをサポートしているように見えますが、現在のリリースのセキュリティ アプライアンスでは同時に 1 台のサーバのみがサポートされます。

構文の説明

hostname	Zone Labs Integrity ファイアウォール サーバのホスト名を指定します。ホスト名のガイドラインについては、**name** コマンドを参照してください。
ip-address	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

コマンド デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このリリースでは、1 台の Zone Labs Integrity ファイアウォール サーバを設定できます。そのサーバで障害が発生した場合は、まず別の Integrity サーバを設定してからクライアント VPN セッションを再確立します。

サーバをホスト名で指定するには、まず **name** コマンドを使用して Zone Labs サーバ名を設定する必要があります。**name** コマンドを使用する前に、**names** コマンドを使用してコマンドをイネーブルにします。

（注）　現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 にサーバ名 ZL-Integrity-Svr を割り当て、その名前を使用して Zone Labs Intergity サーバを設定する例を示します。

```
hostname(config)# names
hostname(config)# name 10.0.0.5 ZL-Integrity-Svr
hostname(config)# zonelabs-integrity server-address ZL-Integrity-Svr
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスが VPN クライアント接続を閉じるように指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-certificate-port

SSL 証明書を取得する場合に Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-certificate-port** コマンドを使用します。デフォルト ポート番号（80）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

構文の説明

cert-port-number	SSL 証明書を要求する場合に Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポート番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは SSL 証明書をセキュリティ アプライアンスのポート 80 で要求します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。**zonelabs-integrity ssl-certificate-port** コマンドで、Zone Labs サーバが SSL サーバ証明書を要求する場合に接続するポートを指定します。

例

次に、セキュリティ アプライアンスのポート 30 で Zone Labs Integrity サーバから SSL 証明書要求を受信するように設定する例を示します。

```
hostname(config)# zonelabs-integrity ssl-certificate-port 30
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-client-authentication

Zone Labs Integrity ファイアウォール サーバの SSL 証明書をセキュリティ アプライアンスで認証できるようにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-client-authentication** コマンドを *enable* 引数を指定して使用します。Zone Labs の SSL 証明書の認証をディセーブルにするには、*disable* 引数を使用するか、またはこのコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

構文の説明

enable	セキュリティ アプライアンスで Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証することを指定します。
disable	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバの SSL 証明書のセキュリティ アプライアンスによる認証はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。ただし、クライアント証明書の認証は任意です。Zone Labs サーバの（SSL クライアント）証明書のセキュリティ アプライアンスによる認証をイネーブルまたはディセーブルにするには、**zonelabs-integrity ssl-client-authentication** コマンドを使用します。

例

次に、Zone Labs Integrity サーバの SSL 証明書を認証するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/