CHAPTER 23

queue-limit コマンド～ rtp-conformance コマンド

queue-limit（プライオリティ キュー）

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

構文の説明

number-of-packets	キューイング（バッファリング）可能な低遅延または通常のプライオリティのパケットの最大数を指定します。この最大数を超えると、インターフェイスでパケットのドロップが開始されます。指定可能な値の範囲については、「使用上のガイドライン」の項を参照してください。

デフォルト

デフォルトのキューの制限は 1024 パケットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、遅延の影響を受けやすい、プライオリティの高いトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）と、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）の 2 つのトラフィック クラスを使用できます。セキュリティ アプライアンスは、プライオリティ トラフィックを認識して、適切な Quality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にする前に、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューを作成する必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドで、プライオリティ キュー モードを開始します。これはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびパケットをドロップする前にバッファに入れることができる両タイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

（注）　インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する*必要があります*。

指定する tx-ring-limit および queue-limit は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの 2 つのパラメータを調整することで、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが、*テールドロップ*です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注）　**queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時にダイナミックに決定されます。この制限を表示するには、コマンド ラインに **help** または **?** と入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論的な最大パケット数は、2147483647 です。

ASA モデル 5505（のみ）では、1 つのインターフェイスにプライオリティ キューを設定すると、他のすべてのインターフェイスで同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけが、すべてのインターフェイスに存在することになります。さらに、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスからも削除されます。

この問題を回避するには、**priority-queue** コマンドを 1 つのインターフェイスにのみ設定します。**queue-limit** コマンドと **tx-ring-limit** コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。

コマンド	説明
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティ キュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。

queue-limit（tcp マップ）

TCP 接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を設定するには、tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

queue-limit *pkt_num* [**timeout** *seconds*]

no queue-limit

構文の説明

pkt_num	TCP 接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を 1 ～ 250 の範囲で指定します。デフォルトは 0 です。この値は、この設定がディセーブルであり、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されることを意味しています。詳細については、「使用上のガイドライン」の項を参照してください。
timeout *seconds*	（任意）順序が不正なパケットをバッファ内に保持可能な最大時間を 1 ～ 20 秒の範囲で設定します。デフォルトは 4 秒です。パケットの順序が不正であり、このタイムアウト期間内に渡されなかった場合、それらのパケットはドロップされます。*pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、制限を 1 以上に設定する必要があります。

デフォルト

デフォルト設定は 0 です。この値は、このコマンドがディセーブルであることを意味しています。

デフォルトのタイムアウトは 4 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)/8.0(4)	**timeout** キーワードが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。

   a. **queue-limit** : tcp マップ コンフィギュレーション モードでは、**queue-limit** コマンドおよびその他数多くのコマンドを入力できます。

2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

TCP 正規化をイネーブルにしない場合、または **queue-limit** コマンドがデフォルトの 0 に設定されている場合（つまりコマンドがディセーブルの場合）、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されます。

- アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP インスペクション再送信（TCP マップ **check-retransmission** コマンド）のための接続のキュー制限は、3 パケットです。セキュリティ アプライアンスが異なるウィンドウ サイズの TCP パケットを受信した場合、キュー制限は、アドバタイズされた設定に合うようにダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

queue-limit コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、TCP パケットからアドバタイズされたすべての設定が**キュー制限**設定を優先して、無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

例

次に、すべての Telnet 接続のキュー制限を 8 パケットに、バッファ タイムアウトを 6 秒に設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8 timeout 6
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

quit

現在のコンフィギュレーション モードを終了したり、特権 EXEC モードやユーザ EXEC モードからログアウトするには、**quit** コマンドを使用します。

quit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **quit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする例を示します。

```
hostname(config)# quit
hostname# quit

Logoff
```

次に、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
hostname(config)# quit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
exit	コンフィギュレーション モードを終了するか、または特権 EXEC モードやユーザ EXEC モードからログアウトします。

radius-common-pw

このセキュリティ アプライアンス経由で特定の RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通パスワードを指定するには、AAA サーバ ホスト モードで **radius-common-pw** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

radius-common-pw *string*

no radius-common-pw

構文の説明

string	この RADIUS サーバにおけるすべての認可トランザクションで共通パスワードとして使用される最大 127 文字の英数字キーワード。大文字と小文字は区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで追加されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバに対してのみ有効です。

RADIUS 認可サーバでは、各接続ユーザに対してパスワードおよびユーザ名が必要です。セキュリティ アプライアンスでは、ユーザ名が自動的に指定されます。ここでは、パスワードを入力します。RADIUS サーバ管理者は、このセキュリティ アプライアンス経由で RADIUS サーバに対して認可を行う各ユーザにこのパスワードが関連付けられるように RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に伝えてください。

共通ユーザ パスワードを指定しない場合、各ユーザのパスワードは各自のユーザ名となります。たとえば、ユーザ名が「jsmith」のユーザは、「jsmith」と入力します。共通ユーザ パスワードにユーザ名を使用する場合は、セキュリティ上の予防措置として、ネットワーク上の他のいずれの場所でもこの RADIUS サーバを認可に使用しないでください。

（注） このフィールドは、実質的には意味がありません。RADIUS サーバはこのフィールドを要求しますが、実際には使用されません。ユーザはこのことを知っている必要はありません。

例

次に、ホスト「1.2.3.4」に「svrgrp1」という名前の RADIUS AAA サーバ グループを設定し、タイムアウト時間を 9 秒に、再試行間隔を 7 秒に、RADIUS 共通パスワードを「allauthpw」に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

radius-reject-message

認証が拒否された場合のログイン画面での RADIUS 拒否メッセージの表示をイネーブルにするには、トンネル グループ webvpn 属性コンフィギュレーション モードで **radius-eject-message** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

radius-reject-message

no radius-reject-message

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

リモート ユーザに対して、認証の失敗についての RADIUS メッセージを表示する場合は、このコマンドをイネーブルにします。

例

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry（削除）

認証中に MS-CHAPv2 を使用してユーザとパスワード アップデートをネゴシエートするようにセキュリティ アプライアンスを設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **radius-with-expiry** コマンドを使用します。RADIUS 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドは無視されます。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

radius-with-expiry

no radius-with-expiry

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換えられました。**radius-with-expiry** コマンドの **no** 形式はサポートされなくなりました。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。

例

次に、設定 ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループに対して radius-with-expiry を設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# radius-with-expiry
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
password-management	パスワード管理をイネーブルにします。**radius-with-expiry** コマンドは、トンネル グループ一般属性コンフィギュレーション モードのこのコマンドに置き換えられました。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

ras-rcf-pinholes

ゲートキーパーがネットワーク内にある場合に、H.323 エンドポイント間でのコール設定をイネーブルにするには、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ras-rcf-pinholes enable

no ras-rcf-pinholes enable

構文の説明

enable	H.323 エンドポイント間でのコール設定をイネーブルにします。

デフォルト

デフォルトでは、このオプションは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスには、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、セキュリティ アプライアンスは発信元 IP アドレス / ポート 0/0 を通じてピンホールを開きます。

例

次に、ポリシー マップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ras-rcf-pinholes enable
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

rate-limit

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **rate-limit** コマンドを使用して、**match** コマンドまたはクラス マップに一致するパケットのメッセージのレートを制限します。このレート制限アクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでこのアクションが可能なわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

構文の説明

messages_per_second	1 秒あたりのメッセージ数を制限します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**rate-limit** コマンドを入力して、メッセージのレートを制限できます。

レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。ここで dns_policy_map はインスペクション ポリシー マップの名前です。

例

次に、invite 要求を 1 秒あたり 100 メッセージに制限する例を示します。

```
hostname(config-cmap)# policy-map type inspect sip sip-map1
hostname(config-pmap-c)# match request-method invite
hostname(config-pmap-c)# rate-limit 100
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

reactivation-mode

グループ内の障害が発生したサーバを再アクティブ化する方法を指定するには、AAA サーバ プロトコル モードで **reactivation-mode** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

構文の説明

deadtime *minutes*	（任意）グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバが非アクティブになった後でのみ、障害が発生したサーバを再アクティブ化します。
timed	30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

デフォルト

デフォルトの再アクティブ化モードは depletion で、デフォルトの deadtime の値は 10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各サーバ グループには、所属するサーバの再アクティブ化ポリシーを指定する属性があります。

depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。**depletion** モードが使用されている場合は、**deadtime** パラメータも指定できます。**deadtime** パラメータは、グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を分単位で指定します。このパラメータは、サーバ グループがローカル フォールバック機能とともに使用されている場合にのみ意味があります。

timed モードでは、障害が発生したサーバは、30 秒のダウン時間の後に再アクティブ化されます。このモードは、サーバ リスト内の最初のサーバをプライマリ サーバとして使用しており、このサーバを可能な限りオンラインに維持する必要がある場合に役立ちます。このポリシーは、UDP サーバの場合

は機能しません。UDP サーバへの接続は、たとえそのサーバが存在しない場合でも失敗しないため、UDP サーバは無条件にオンラインに戻ります。サーバ リストに到達不能な複数のサーバが含まれている場合には、接続時間が遅延したり、接続に失敗する場合があります。

同時アカウンティングがイネーブルになっているアカウンティング サーバ グループでは、**timed** モードが強制的に使用されます。このことは、特定のリスト内のすべてのサーバが同等に扱われることを意味しています。

例

次に、「srvgrp1」という名前の TACACS+ AAA サーバで、再アクティブ化モードを depletion に、deadtime を 15 分に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

次に、「srvgrp1」という名前の TACACS+ AAA サーバで timed 再アクティブ化モードを使用するように設定する例を示します。

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)#
```

関連コマンド

accounting-mode	アカウンティング メッセージが単一のサーバに送信されるか、またはグループ内のすべてのサーバに送信されるかを示します。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始して、グループ内のすべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できるようにします。
max-failed-attempts	サーバ グループ内の所定のサーバが非アクティブ化されるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

record-entry

CTL ファイルの作成に使用されるトラストポイントを指定するには、CTL ファイル コンフィギュレーション モードで record-entry コマンドを使用します。CTL からレコード エントリを削除するには、このコマンドの **no** 形式を使用します。

record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

no record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trust_point* **address** *ip_address* [**domain-name** *domain_name*]

構文の説明

capf	このトラストポイントのロールを CAPF に指定します。1 つの CAPF トラストポイントのみを設定できます。
cucm	このトラストポイントのロールを CCM に指定します。複数の CCM トラストポイントを設定できます。
cucm-tftp	このトラストポイントのロールを CCM+TFTP に指定します。複数の CCM+TFTP トラストポイントを設定できます。
domain-name *domain_name*	（任意）トラストポイントの DNS フィールドの作成に使用されるトラストポイントのドメイン名を指定します。この名前は、サブジェクト DN の一般名フィールドに追加されて、DNS 名が作成されます。トラストポイントに FQDN が設定されていない場合は、ドメイン名を設定する必要があります。
address *ip_address*	トラストポイントの IP アドレスを指定します。
tftp	このトラストポイントのロールを TFTP に指定します。複数の TFTP トラストポイントを設定できます。
trustpoint *trust_point*	インストールされているトラストポイントの名前を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

domain-name は、1 つのみ指定できます。CTL ファイルが存在しない場合は、手動でこの証明書を CUCM からセキュリティ アプライアンスにエクスポートします。

このコマンドは、電話プロキシの CTL ファイルを設定していない場合にのみ使用します。すでに CTL ファイルを設定している場合は、このコマンドを使用しないでください。

ip_address 引数に指定する IP アドレスは、トラストポイントの CTL レコードで使用される IP アドレスとなるため、グローバル アドレス、または IP Phone によって認識されるアドレスである必要があります。

CTL ファイルで必要な各エントリに対して、さらに record-entry コンフィギュレーションを追加します。

例

次に、**record-entry** コマンドを使用して、CTL ファイルの作成に使用されるトラストポイントを指定する例を示します。

```
hostname(config-ctl-file)# record-entry cucm-tftp trustpoint cucm1 address 192.168.1.2
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

redirect-fqdn

VPN ロード バランシング モードで完全修飾ドメイン名を使用したリダイレクトをイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。

redirect-fqdn {enable | disable}

no redirect-fqdn {enable | disable}

（注） VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

disable	完全修飾ドメイン名を使用したリダイレクトをディセーブルにします。
enable	完全修飾ドメイン名を使用したリダイレクトをイネーブルにします。

デフォルト

この動作は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。

VPN クラスタ マスターとして、セキュリティ アプライアンスは、VPN クライアント接続を別のクラスタ デバイスにリダイレクトする場合に、DNS 逆ルックアップを使用して、そのクラスタ デバイス（クラスタ内の別のセキュリティ アプライアンス）の外部 IP アドレスではなく Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく FQDN を使用して WebVPN ロード バランシングを実行するには、次の設定手順を実行する必要があります。

ステップ 1　**redirect-fqdn enable** コマンドを使用して、ロード バランシングにおける FQDN の使用をイネーブルにします。

ステップ 2　DNS サーバに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。

ステップ 3　dns domain-lookup inside コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバへのルートを持つ任意のインターフェイスを指定します。

ステップ 4　`dns name-server 10.2.3.4` のように、ASA に DNS サーバの IP アドレスを定義します（10.2.3.4 は、DNS サーバの IP アドレス）。

例

次に、リダイレクトをディセーブルにする **redirect-fqdn** コマンドの例を示します。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn disable
hostname(config-load-balancing)#
```

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを「test」と指定し、クラスタのプライベート インターフェイスを「foo」と指定するインターフェイス コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロード バランシング仮想クラスタのコンフィギュレーションを表示します。

コマンド	説明
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

redistribute（EIGRP）

1 つのルーティング ドメインから EIGRP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

構文の説明

bandwidth	EIGRP 帯域幅メトリック（キロビット/秒）。有効な値は、1 ～ 4294967295 です。
connected	インターフェイスに接続されているネットワークを EIGRP ルーティング プロセスに再配布することを指定します。
delay	EIGRP 遅延メトリック（10 マイクロ秒単位）有効な値は、0 ～ 4294967295 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
load	EIGRP 有効帯域幅（負荷）メトリック。有効な値は、1 ～ 255 です（255 は 100% の負荷を示します）。
match	（任意）OSPF から EIGRP にルートを再配布する条件を指定します。
metric	（任意）EIGRP ルーティング プロセスに再配布されるルートの EIGRP メトリックの値を指定します。
mtu	パスの MTU。有効な値は 1 ～ 65535 です。
nssa-external *type*	NSSA の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	EIGRP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
reliability	EIGRP 信頼性メトリック。有効な値は、0 ～ 255 です（255 は 100% の信頼性を示します）。
rip	RIP ルーティング プロセスから EIGRP ルーティング プロセスへのネットワークの再配布を指定します。
route-map *map_name*	（任意）送信元ルーティング プロトコルから EIGRP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルートマップの名前。指定しない場合は、すべてのルートが再配布されます。
static	EIGRP ルーティング プロセスにスタティック ルートを再配布するために使用します。

デフォルト

コマンドのデフォルトは次のとおりです。

- **match**：**Internal**、**external 1**、**external 2**

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン　EIGRP コンフィギュレーションに **default-metric** コマンドを設定していない場合は、redistribute コマンドで **metric** を指定する必要があります。

例　次に、スタティック ルートおよび接続ルートを EIGRP ルーティング プロセスに再配布する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# redistribute static
hostname(config-router)# redistribute connected
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（OSPF）

1 つのルーティング ドメインから OSPF ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected** | **eigrp** *as-number*} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

構文の説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	OSPF ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効な値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を指定します。
metric *metric_value*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type *metric_type*	（任意）OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられている外部リンク タイプ。**1**（タイプ 1 外部ルート）または **2**（タイプ 2 外部ルート）を指定できます。
nssa-external *type*	NSSA の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	現在の OSPF ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
rip	RIP ルーティング プロセスから現在の OSPF ルーティング プロセスへのネットワークの再配布を指定します。
route-map *map_name*	（任意）送信元ルーティング プロトコルから現在の OSPF ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルート マップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。

subnets	（任意）OSPF へのルートの再配布において、指定したプロトコルの再配布の範囲を指定します。使用しない場合は、クラスフル ルートのみが再配布されます。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **metric-type** *type-value*：**2**
- **match**：**Internal**、**external 1**、**external 2**
- **tag** *tag-value*：0

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは、**rip** キーワードを含むように変更されました。
8.0(2)	このコマンドが、**eigrp** キーワードを含めるように修正されました。

例

次に、スタティック ルートを現在の OSPF プロセスに再配布する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute static
```

関連コマンド

コマンド	説明
redistribute（RIP）	RIP ルーティング プロセスにルートを再配布します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redistribute（RIP）

別のルーティング ドメインから RIP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

構文の説明

connected	インターフェイスに接続されているネットワークを RIP ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	RIP ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効な値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）OSPF から RIP にルートを再配布する条件を指定します。
metric {*metric_value* | **transparent**}	（任意）再配布するルートの RIP メトリック値を指定します。*metric_value* の有効な値は、0 ～ 16 です。メトリックを **transparent** に設定すると、現在のルート メトリックが使用されます。
nssa-external *type*	Not-So-Stubby Area（NSSA）の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	RIP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
route-map *map_name*	（任意）送信元ルーティング プロトコルから RIP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルート マップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを RIP プロセスに再配布するために使用されます。

デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **match**：**Internal**、**external 1**、**external 2**

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	このコマンドが、**eigrp** キーワードを含めるように修正されました。

例　次に、スタティック ルートを現在の RIP プロセスに再配布する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# redistribute static metric 2
```

関連コマンド

コマンド	説明
redistribute（EIGRP）	他のルーティング ドメインから EIGRP にルートを再配布します。
redistribute（OSPF）	他のルーティング ドメインから OSPF にルートを再配布します。
router rip	RIP ルーティング プロセスをイネーブルにして、そのプロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

redundant-interface

冗長インターフェイスのうちのどのメンバー インターフェイスをアクティブにするかを設定するには、特権 EXEC モードで **redundant-interface** コマンドを使用します。

redundant-interface redundant*number* **active-member** *physical_interface*

構文の説明

active-member *physical_interface*	アクティブ メンバーを設定します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。
redundant*number*	冗長インターフェイス ID（**redundant1** など）を指定します。

デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバー インターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

```
hostname# show interface redundantnumber detail | grep Member
```

次に例を示します。

```
hostname# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

例

次に、冗長インターフェイスを作成する例を示します。デフォルトでは、gigabitethernet 0/0 がコンフィギュレーション内の最初のインターフェイスであるため、このインターフェイスがアクティブです。redundant-interface コマンドでは、gigabitethernet 0/1 をアクティブ インターフェイスに設定しています。

```
hostname(config-if)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1

hostname(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
member-interface	冗長インターフェイス ペアにメンバー インターフェイスを割り当てます。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

regex

テキストを照合する正規表現を作成するには、グローバル コンフィギュレーション モードで **regex** コマンドを使用します。正規表現を削除するには、このコマンドの **no** 形式を使用します。

regex *name regular_expression*

no regex *name* [*regular_expression*]

構文の説明

name	正規表現名を最大 40 文字で指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

regex コマンドは、テキスト照合が必要なさまざまな機能で使用できます。たとえば、*インスペクション ポリシー マップ*を使用して、モジュラ ポリシー フレームワーク を使用したアプリケーション インスペクションの特別なアクションを設定できます（**policy map type inspect** コマンドを参照）。インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラス マップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現は、正規表現クラス マップにグループ化できます（**class-map type regex** コマンドを参照）。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。正規表現を使用して、特定のアプリケーション トラフィックの内容（HTTP パケット内の本文テキストなど）を照合できます。

（注） 最適化のために、セキュリティ アプライアンスでは、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。「http://」などの、一般的に 2 つのスラッシュが使用されるストリングでは、代わりに「http:/」を検索してください。

表 23-1 に、特別な意味を持つメタ文字の一覧を示します。

表 23-1　regex メタ文字

文字	説明	注意事項
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp***)**	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 **（注）** Ctrl+V を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x*} または {*x*,}	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^*abc***]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は、a、b、c 以外の任意の文字に一致します。**[^A-Z]** は、大文字のアルファベット文字以外の任意の単一の文字に一致します。

表 23-1　regex メタ文字 （続き）

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

正規表現が想定どおりに一致するかどうかをテストするには、**test regex** コマンドを入力します。

正規表現のパフォーマンスへの影響は、主に次の 2 つの要因によって決定されます。

- 正規表現照合で検索される必要があるテキストの長さ。

  検索長が短い場合は、正規表現エンジンのセキュリティ アプライアンスに対するパフォーマンス上の影響は小さくなります。

- 正規表現照合で検索される必要がある正規表現チェーン テーブルの数。

検索長のパフォーマンスへの影響

正規表現検索を設定すると、通常は、検索対象テキストのすべてのバイトが正規表現データベースに対して検査されて、一致が検索されます。検索対象テキストが長くなるほど、検索時間も長くなります。次に、この現象を表すパフォーマンス テスト ケースを示します。

- ある HTTP トランザクションでは、1 回の 300 バイトの GET 要求と 1 回の 3250 バイトの応答が行われます。
- URI 検索には 445 の正規表現が、要求本文検索には 34 の正規表現が使用されます。
- 応答本文検索には 55 の正規表現が使用されます。

URI および HTTP GET 要求の本文のみを検索するようにポリシーを設定すると、スループットは次のようになります。

- 対応する正規表現データベースが検索されない場合は 420 mbps。
- 対応する正規表現データベースが検索される場合は 413 mbps（正規表現を使用するオーバーヘッドが比較的小さいことがわかります）。

ただし、HTTP 応答本文全体も検索するようにポリシーを設定すると、応答本文の検索対象が長いため（3250 バイト）、スループットは 145 mbps まで低下します。

正規表現検索のテキスト長が長くなる要因は次のとおりです。

- 複数の異なるプロトコル フィールドに対して正規表現検索が設定されている場合。たとえば、HTTP インスペクションでは、URI にのみ正規表現照合が設定されていると、URI フィールドのみが正規表現照合のために検索され、検索長は URI 長に制限されます。ただし、ヘッダーや本文などの他のプロトコル フィールドにも正規表現照合が設定されていると、ヘッダー長や本文長の分だけ検索長が長くなります。
- 検索対象のフィールドが長い場合。たとえば、URI に正規表現検索が設定されている場合、GET 要求内の長い URI の検索長は長くなります。また、現在、HTTP 本文の検索長はデフォルトで 200 バイトまでに制限されています。ただし、本文を検索するようにポリシーを設定し、本文検索長が 5000 バイトに変更されると、本文検索が長くなるため、パフォーマンスに対して大きな影響があります。

正規表現チェーン テーブル数のパフォーマンスへの影響

現在、同じプロトコル フィールドに設定されたすべての正規表現（URI に対するすべての正規表現など）は、1 つ以上の正規表現チェーン テーブルで構成されるデータベースに構築されます。テーブルの数は、必要な合計メモリ量、およびテーブル構築時に使用可能なメモリ量によって決定されます。次のいずれかの条件が満たされる場合、正規表現データベースは複数のテーブルに分割されます。

- 必要な合計メモリが 32 MB を超える場合。これは、最大テーブル サイズが 32 MB に制限されているためです。
- 最大連続メモリ サイズが正規表現データベース全体を構築するのに十分ではない場合、複数の小さなテーブルが構築されて、それらのテーブルにすべての正規表現が格納されます。メモリ フラグメンテーションの程度は、相互に関連する数多くの要因によって左右されるため、フラグメンテーションのレベルを予測することは事実上不可能です。

複数のチェーン テーブルがある場合、正規表現照合において各テーブルが検索される必要があるため、検索時間は検索対象のテーブル数に比例して長くなります。

特定のタイプの正規表現では、テーブル サイズが大幅に増加する傾向があります。可能な限りワイルドカードおよび繰り返し要素を避けるように正規表現を設計することを推奨します。次のメタ文字については、表 23-1 を参照してください。

- ワイルドカード タイプの指定を伴う正規表現
  - ドット（.）
- クラス内の任意の文字に一致するさまざまな文字クラス
  - [^a-z]
  - [a-z]
  - [abc]]
- 繰り返しタイプの指定を伴う正規表現
  - *
  - +
  - {n,}

- 次のようにワイルドカード タイプの正規表現と繰り返しタイプの正規表現を組み合わせると、テーブル サイズが大幅に増加する可能性があります。
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.*（これは、「123」と照合することと同じであるため、このような指定は行わないでください）。

次に、ワイルドカードや繰り返しの有無によって正規表現のメモリ使用量がどのように異なるかについての例を示します。

- 次の 4 つの正規表現のデータベース サイズは 958,464 バイトです。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 次の 4 つの正規表現のデータベース サイズはわずか 10240 バイトです。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

正規表現の数が増えると、正規表現データベースで必要になる合計メモリ量も増え、そのためメモリがフラグメント化されている場合にはより多くのテーブル数が必要になる可能性があります。次に、異なる正規表現数でのメモリ使用量の例を示します。

- 100 サンプル URI : 3,079,168 バイト
- 200 サンプル URI : 7,156,224 バイト
- 500 サンプル URI : 11,198,971 バイト

（注） コンテキストごとの最大正規表現数は 2048 です。

debug menu regex 40 10 コマンドを使用して、各正規表現データベースにおけるチェーン テーブル数を表示できます。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックと照合するインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。

コマンド	説明
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
test regex	正規表現をテストします。

reload

リブートしてコンフィギュレーションをリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm*] [**max-hold-time** [*hh*:]*mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

構文の説明

at *hh*:*mm*	（任意）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定しない場合、リロードは、指定時刻が現在時刻よりも後の場合は当日の指定時刻に、指定時刻が現在時刻よりも前の場合は翌日の指定時刻に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 時間以内に実行される必要があります。
cancel	（任意）スケジューリングされているリロードをキャンセルします。
day	（任意）1 ～ 31 の範囲で日付を指定します。
in [*hh*:]*mm*]	（任意）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、24 時間以内に実行される必要があります。
max-hold-time [*hh*:]*mm*	（任意）シャットダウンまたはリブートの前に他のサブシステムに対して通知するためにセキュリティ アプライアンスが待機する最大ホールド タイムを指定します。この時間が経過すると、（強制）クイック シャットダウンまたはリブートが実行されます。
month	（任意）月の名前を指定します。月の名前を表す一意のストリングを作成するために十分な文字を入力します。たとえば、「Ju」は、June または July を表すことができるため一意ではありませんが、「Jul」は一意です。これは、「Jul」で始まる月は「July」しかないためです。
noconfirm	（任意）ユーザの確認なしでリロードすることをセキュリティ アプライアンスに許可します。
quick	（任意）すべてのサブシステムに対して通知や適切なシャットダウンを行わないで、強制的にクイック リロードを行います。
reason *text*	（任意）リロードの理由を 1 ～ 255 文字で指定します。理由のテキストは、すべての開いている IPSec VPN クライアント、端末、コンソール、telnet、SSH、および ASDM 接続またはセッションに送信されます。 **（注）** isakmp などの一部のアプリケーションでは、IPSec VPN クライアントに理由のテキストを送信するために追加のコンフィギュレーションが必要となります。詳細については、ソフトウェア コンフィギュレーション マニュアルの該当する項を参照してください。
save-config	（任意）シャットダウンの前に、実行コンフィギュレーションをメモリに保存します。**save-config** キーワードを入力しない場合、未保存のコンフィギュレーションの変更はリロード後にすべて失われます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されて、*day*、*hh*、*mm*、*month*、**quick**、**save-config**、および *text* という新しい引数およびキーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンス がリブートし、フラッシュからコンフィギュレーションがリロードされます。

デフォルトで、**reload** コマンドは対話形式です。セキュリティ アプライアンスは、まずコンフィギュレーションが変更されており、未保存であるかどうかをチェックします。変更が未保存の場合、コンフィギュレーションを保存するように求めるプロンプトがセキュリティ アプライアンスによって表示されます。マルチ コンテキスト モードでは、セキュリティ アプライアンスによって、未保存のコンフィギュレーションがある各コンテキストに対してプロンプトが表示されます。**save-config** パラメータを指定すると、コンフィギュレーションはプロンプトなしで保存されます。次に、システムのリロードを確認するプロンプトがセキュリティ アプライアンスによって表示されます。**y** と入力するか、または Enter キーを押した場合にのみリロードが行われます。確認後、セキュリティ アプライアンスは、遅延パラメータ（**in** または **at**）を指定したかどうかに応じて、リロード プロセスを開始またはスケジューリングします。

デフォルトで、リロード プロセスは「グレースフル」（「ナイス」とも呼ばれます）モードで動作します。すべての登録されているサブシステムは、リブート実行の前に通知されるため、リブート前に適切にシャットダウンできます。このようなシャットダウンが行われるのを待機しない場合は、**max-hold-time** パラメータを指定して、待機する最大時間を指定します。または、**quick** パラメータを使用して、影響のあるサブシステムへの通知やグレースフル シャットダウンの待機を行わずに、すぐに強制的にリロード プロセスを開始できます。

noconfirm パラメータを指定すると、**reload** コマンドを非対話形式で実行できます。この場合、セキュリティ アプライアンスでは、**save-config** パラメータを指定していない限り、未保存のコンフィギュレーションがあるかどうかはチェックされません。また、セキュリティ アプライアンスでは、システムのリブート前にユーザに対して確認を求めるプロンプトは表示されません。遅延パラメータを指定していない限り、リロード プロセスがすぐに開始またはスケジューリングされます。ただし、**max-hold-time** パラメータまたは **quick** パラメータを指定して、動作またはリロード プロセスを制御できます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** を使用します。すでに進行中のリロードはキャンセルできません。

（注） フラッシュ パーティションに書き込まれていない設定変更は、リロード後に失われます。リブート前に、**write memory** コマンドを入力して、現在の設定をフラッシュ パーティションに保存してください。

例

次の例は、コンフィギュレーションをリブートおよびリロードする方法を示しています。

```
hostname# reload
```

```
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	セキュリティ アプライアンスのリロード ステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモート アクセス セッションの数を指定します。この数を超えると、セキュリティ アプライアンスによってトラップが送信されます。

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

構文の説明

threshold-value	セキュリティ アプライアンスでサポートされるセッションの制限数以下の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0 (1)	このコマンドが導入されました。

例

次に、しきい値を 1500 に設定する例を示します。

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値によるトラッピングをイネーブルにします。

rename

ファイルまたはディレクトリの名前をある名前から別の名前に変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename ***[/noconfirm] [***disk0: | disk1: | flash:***]*** *source-path* **[**disk0: | disk1: | flash:***]*** *destination-path*

構文の説明

/noconfirm	（任意）確認プロンプトを表示しないようにします。
destination-path	新しいファイル名のパスを指定します。
disk0:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
source-path	元のファイル名のパスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

rename flash: flash: コマンドを入力すると、元のファイル名および新しいファイル名を入力するように求められます。

ファイル システムにまたがってファイルやディレクトリの名前を変更することはできません。

次に例を示します。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次に、「test」というファイル名を「test1」に変更する例を示します。

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイル システムに関する情報を表示します。

rename（クラス マップ）

クラス マップの名前を変更するには、クラス マップ コンフィギュレーション モードで **rename** コマンドを入力します。

rename *new_name*

構文の説明

new_name	クラス マップの新しい名前を最大 40 文字で指定します。「class-default」という名前は予約されています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、test というクラス マップの名前を test2 に変更する例を示します。

```
hostname(config)# class-map test
hostname(config-cmap)# rename test2
```

関連コマンド

コマンド	説明
class-map	クラス マップを作成します。

renewal-reminder

ローカルの Certificate Authority（CA; 認証局）証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定するには、CA サーバ コンフィギュレーション モードで **renewal-reminder** コマンドを使用します。期間をデフォルトの 14 日にリセットするには、このコマンドの **no** 形式を使用します。

renewal-reminder *time*

no renewal-reminder

構文の説明

time	発行されている証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定します。有効な値の範囲は、1 ～ 90 日です。

デフォルト

デフォルトで、CA サーバは、証明書が期限切れになる 14 日前に再登録を求める有効期限通知およびリマインダを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

証明書有効期限 - 更新リマインダ日数の時点、（有効期限 + ワンタイム パスワード有効期限）- 更新リマインダ日数 / 2 の時点、および（有効期限 + ワンタイム パスワード有効期限）- 更新リマインダ日数 / 4 の時点の合計 3 回のリマインダが送信されます。

ユーザ データベースに電子メール アドレスが指定されている場合は、3 回の各リマインダにおいて、電子メールが証明書所有者に自動的に送信されます。電子メール アドレスが存在しない場合は、更新を管理者に通知する syslog メッセージが生成されます。

例

次に、証明書有効期限の 7 日前にセキュリティ アプライアンスからユーザに対して有効期限通知を送信するように指定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# renewal-reminder 7
hostname(config-ca-server)#
```

次に、有効期限通知のタイミングをデフォルトである証明書有効期限の 14 日前にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no renewal-reminder
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
lifetime	CA 証明書、すべての発行されている証明書、および CRL のライフタイムを指定します。
show crypto ca server	ローカル CA サーバのコンフィギュレーション詳細を表示します。

replication http

フェールオーバー グループに対して HTTP 接続のレプリケーションをイネーブルにするには、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

replication http

no replication http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**replication http** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー コンフィギュレーションのフェールオーバー グループに対するコマンドであることを除いて、Active/Standby フェールオーバー用の **failover replication http** コマンドと同じ機能を備えています。

例

次の例では、フェールオーバー グループで可能な設定を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover replication http	HTTP 接続を複製するためのステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内の特定のコマンドを禁止するには、FTP マップ コンフィギュレーション モードで **request-command deny** コマンドを使用します。FTP マップ コンフィギュレーション モードには、**ftp-map** コマンドを使用してアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

構文の説明

appe	ファイルへの追加を行うコマンドを拒否します。
cdup	現在の作業ディレクトリの親ディレクトリに移動するコマンドを拒否します。
dele	サーバのファイルを削除するコマンドを拒否します。
get	サーバからファイルを取得するクライアント コマンドを拒否します。
help	ヘルプ情報を提供するコマンドを拒否します。
mkd	サーバ上にディレクトリを作成するコマンドを拒否します。
put	サーバにファイルを送信するクライアント コマンドを拒否します。
rmd	サーバ上のディレクトリを削除するコマンドを拒否します。
rnfr	変更元ファイル名を指定するコマンドを拒否します。
rnto	変更先ファイル名を指定するコマンドを拒否します。
site	サーバ システムに固有のコマンドを禁止します。通常、リモート管理に使用します。
stou	固有のファイル名を使用してファイルを保存するコマンドを拒否します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ストリクト FTP インスペクションを使用する場合に、セキュリティ アプライアンスを通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例

次に、**stor**、**stou**、または **appe** コマンドを含む FTP 要求をセキュリティ アプライアンスでドロップする例を示します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。
mask-syst-reply	FTP サーバ応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

request-data-size

SLA 動作要求パケットのペイロードのサイズを設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **request-data-size** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-data-size *bytes*

no request-data-size

構文の説明

bytes	要求パケットのペイロードのサイズ（バイト単位）。有効な値は、0 ～ 16384 です。最小値は、使用するプロトコルに応じて異なります。エコー タイプでは、最小値は 28 バイトです。プロトコルまたは PMTU で許可されている最大値よりも大きい値を設定しないでください。 **（注）** セキュリティ アプライアンスによって 8 バイトのタイムスタンプがペイロードに追加されるため、実際のペイロードは *bytes* + 8 バイトになります。

デフォルト

デフォルトの *bytes* は 28 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

到達可能性を確保するために、デフォルトのデータ サイズを大きくして、送信元と宛先との間の PMTU の変化を検出する必要がある場合があります。PMTU が低いと、セッションのパフォーマンスに影響を与える可能性が高くなります。また、低い PMTU が検出された場合は、セカンダリ パスが使用されることを示している可能性があります。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
```

```
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

request-queue

応答を待機する GTP 要求のキューイング可能最大数を指定するには、GTP マップ コンフィギュレーション モードで **request-queue** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスします。この数字をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*

no request-queue *max_requests*

構文の説明

max_requests	応答を待機する GTP 要求のキューイング可能最大数。値の範囲は、1 ～ 4294967295 です。

デフォルト

max_requests のデフォルトは 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gtp request-queue コマンドは、応答を待機する GTP 要求のキューイング可能最大数を指定します。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。

例

次に、300 バイトの最大要求キュー サイズを指定する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

request-timeout

失敗した SSO 認証試行がタイムアウトになるまでの秒数を設定するには、webvpn コンフィギュレーション モードで **request-timeout** コマンドを使用します。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-timeout *seconds*

no request-timeout

構文の説明

seconds	失敗した SSO 認証の試行がタイムアウトするまでの秒数。指定できる範囲は 1 ～ 30 秒です。小数の値はサポートされていません。

デフォルト

このコマンドのデフォルト値は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。現在、セキュリティ アプライアンスでは、SiteMinder-type および SAML POST-type の SSO サーバがサポートされています。

このコマンドは SSO サーバの両タイプに適用されます。

SSO 認証をサポートするようにセキュリティ アプライアンスを設定した後、2 つのタイムアウト パラメータを調整できます。

- 失敗した SSO 認証試行がタイムアウトになるまでの秒数（**request-timeout** コマンドを使用）。
- 失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数（**max-retry-attempts** コマンドを参照）。

例

次に、webvpn 設定 sso siteminder モードで、SiteMinder-type SSO サーバ「example」の認証タイムアウトを 10 秒に設定する例を示します。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# request-timeout 10
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

reserve-port-protect

メディア ネゴシエーション中の予約ポートの使用を制限するには、パラメータ コンフィギュレーション モードで **reserve-port-protect** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

reserve-port-protect

no reserve-port-protect

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、RTSP インスペクション ポリシー マップで予約ポートを保護する例を示します。

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# reserve-port-protect
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

reserved-bits

TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりするには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

構文の説明

allow	TCP ヘッダーの予約ビットが設定されているパケットを許可します。
clear	TCP ヘッダーの予約ビットをクリアして、パケットを許可します。
drop	TCP ヘッダーの予約ビットが設定されているパケットをドロップします。

デフォルト

デフォルトで、予約ビットは許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。末端のホストにおける予約ビットが設定されているパケットの処理方法を明確に指定するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。処理方法が明確に指定されていないと、セキュリティ アプライアンスが同期化されていない状態になる可能性があります。TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりできます。

例

次に、すべての TCP フローにおいて、予約ビットが設定されているパケットをクリアする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

reset

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **reset** コマンドを使用して、**match** コマンドまたはクラス マップに一致するトラフィックに対してパケットをドロップし、接続を閉じて、TCP リセットを送信します。このリセット アクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでこのアクションが可能なわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

reset [**log**]

no reset [**log**]

構文の説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**reset** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するトラフィックに対してパケットをドロップし、接続を閉じることができます。

接続をリセットした後は、インスペクション ポリシー マップのアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドまたは **class** コマンドとの照合は行われません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます 同じ **match** または **class** コマンドに対して **reset** アクションと **log** アクションの両方を設定できます。この場合、パケットは、特定の一致において、ログに記録されてからリセットされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、http-traffic クラス マップに一致した場合に、接続をリセットして、ログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

retries

セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

retries *number*

no retries [*number*]

構文の説明

number	再試行回数を 0 ～ 10 の範囲で指定します。デフォルトは 2 です。

デフォルト

デフォルトの再試行回数は 2 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

name-server コマンドを使用して DNS サーバを追加します。

dns name-server コマンドがこのコマンドに置き換えられました。

例

次に、再試行回数を 0 回に設定する例を示します。セキュリティ アプライアンスは各サーバへの要求を 1 回のみ行います。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns retries 0
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループ モードを開始します。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

retry-interval

指定済みの aaa-server host コマンドで指定されている特定の AAA サーバへの再試行間隔を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。再試行間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

retry-interval *seconds*

no retry-interval

構文の説明

seconds	要求の再試行間隔（1 ～ 10 秒）を指定します。これは、セキュリティ アプライアンスが接続要求を再試行するまでに待機する時間です。

デフォルト

デフォルトの再試行間隔は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは CLI ガイドラインに沿うように変更されました。

使用上のガイドライン

接続試行間にセキュリティ アプライアンスが待機する秒数を指定またはリセットするには、**retry-interval** コマンドを使用します。セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。

例

次に、コンテキストでの **retry-interval** コマンドの例を示します。

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

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。

show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。
timeout	セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定します。

reval-period

NAC フレームワーク セッションにおける成功した各ポスチャ検証間の間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **reval-period** コマンドを使用します。このコマンドを NAC フレームワーク ポリシーから削除するには、このコマンドの **no** 形式を使用します。

reval-period *seconds*

no reval-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 300 ～ 86400 です。

デフォルト

デフォルト値は 36000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ポスチャ検証に成功するたびに、再検証タイマーが開始されます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。セキュリティ アプライアンスでは、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバが使用できない場合、デフォルトのグループ ポリシーが有効になります。

例

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
hostname(config-nac-policy-nac-framework)# reval-period 86400
hostname(config-nac-policy-nac-framework)
```

次に、NAC ポリシーから再検証タイマーを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no reval-period
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。

revert webvpn all

セキュリティ アプライアンス のフラッシュ メモリから、すべての Web 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除するには、特権 EXEC モードで **revert webvpn all** コマンドを入力します。

revert webvpn all

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスのフラッシュ メモリから Web 関連のすべての情報（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）をディセーブルにし、削除するには、**revert webvpn all** コマンドを使用します。すべての Web 関連データを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、セキュリティ アプライアンスからすべての Web 関連コンフィギュレーション データを削除するコマンドを示します。

```
hostname# revert webvpn all
hostname
```

関連コマンド

コマンド	説明
show import webvpn (*任意*)	このコマンドは、セキュリティ アプライアンス上のフラッシュ メモリにそのとき存在する、さまざまなインポートされた WebVPN データおよびプラグインを表示します。

revert webvpn customization

セキュリティ アプライアンスのキャッシュ メモリからカスタマイゼーション オブジェクトを削除するには、特権 EXEC モードで **revert webvpn customization** コマンドを入力します。

revert webvpn customization *name*

構文の説明

name	削除するカスタマイゼーション オブジェクトの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

指定したカスタマイゼーションのリモート クライアントレス SSL VPN サポートを削除し、セキュリティ アプライアンスのキャッシュ メモリからそのカスタマイゼーション オブジェクトを削除するには、**revert webvpn customization** コマンドを使用します。カスタマイゼーション オブジェクトを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。カスタマイゼーション オブジェクトには、特定の指定されたポータル ページのコンフィギュレーション パラメータが含まれています。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションの設定機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。セキュリティ アプライアンスでは、8.0 ソフトウェアへのアップグレード時に、古い設定を使用して新しいカスタマイゼーション オブジェクトを生成することによって、現在の設定が保持されます。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

（注） バージョン 7.2 のポータル カスタマイゼーションおよび URL リストは、バージョン 8.0 へのアップグレード前にバージョン 7.2(x) のコンフィギュレーション ファイルで適切なインターフェイスにおいてクライアントレス SSL VPN（WebVPN）がイネーブルになっている場合にのみ、ベータ 8.0 コンフィギュレーションで動作します。

例

次に、GroupB という名前のカスタマイゼーション オブジェクトを削除するコマンドを示します。

```
hostname# revert webvpn customization groupb
```

```
hostname
```

関連コマンド

コマンド	説明
customization	トンネル グループ、グループ、またはユーザに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	セキュリティ アプライアンスのフラッシュ デバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn plug-in protocol

セキュリティ アプライアンスのフラッシュ デバイスからプラグインを削除するには、特権 EXEC モードで **revert webvpn plug-in protocol** コマンドを入力します。

revert plug-in protocol *protocol*

構文の説明

protocol	次のいずれかのストリングを入力します。 • **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。 • **ssh** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

指定した Java ベースのクライアント アプリケーションのクライアントレス SSL VPN サポートをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ ドライブからも削除するには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次に、RDP のサポートを削除するコマンドを示します。

```
hostname# revert webvpn plug-in protocol rdp
hostname
```

関連コマンド

コマンド	説明
import webvpn plug-in protocol	指定したプラグインを URL からセキュリティ アプライアンスのフラッシュ デバイスにコピーします。このコマンドを発行すると、クライアントレス SSL VPN での今後のセッションにおいて、Java ベースのクライアント アプリケーションの使用が自動的にサポートされます。
show import webvpn plug-in	セキュリティ アプライアンスのフラッシュ デバイスに存在するプラグインのリストを示します。

revert webvpn translation-table

セキュリティ アプライアンスのフラッシュ メモリから変換テーブルを削除するには、特権 EXEC モードで **revert webvpn translation-table** コマンドを入力します。

revert webvpn translation-table *translationdomain language*

構文の説明

translationdomain	使用可能な変換ドメインは、次のとおりです。 • AnyConnect • PortForwarder • バナー • CSD • カスタマイゼーション • URL リスト • （RDP、SSH、および VNC プラグインからのメッセージの変換）
language	削除する文字エンコーディング方法を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

インポートされた変換テーブルをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ メモリからも削除するには、**revert webvpn translation-table** コマンドを使用します。変換テーブルを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、Dutch という AnyConnect 変換テーブルを削除するコマンドを示します。

```
hostname# revert webvpn translation-table anyconnect dutch
hostname
```

関連コマンド

コマンド	説明
revert webvpn all	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn translation-table	セキュリティ アプライアンスのフラッシュ デバイスに存在する現在の変換テーブルを表示します。

revert webvpn url-list

セキュリティ アプライアンスから URL リストを削除するには、特権 EXEC モードで **revert webvpn url-list** コマンドを入力します。

revert webvpn url-list template *name*

構文の説明

template *name*	URL リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスのフラッシュ ドライブから現在の URL リストをディセーブルにし、削除するには、**revert webvpn url-list** コマンドを使用します。URL リストを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

revert webvpn url-list コマンドで使用される template 引数では、設定済みの URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

例

次に、servers2 という URL リストを削除するコマンドを示します。

```
hostname# revert webvpn url-list servers2
hostname
```

関連コマンド

コマンド	説明
revert webvpn all	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show running-configuration url-list	現在の設定済み URL リスト コマンドのセットを表示します。
url-list（**webvpn** モード）	特定のユーザまたはグループ ポリシーに、WebVPN サーバおよび URL のリストを適用します。

revert webvpn webcontent

セキュリティ アプライアンスのフラッシュ メモリ内の場所から指定した Web オブジェクトを削除するには、特権 EXEC モードで **revert webvpn webcontent** コマンドを入力します。

revert webvpn webcontent *filename*

構文の説明

filename	削除する Web コンテンツを含むフラッシュ メモリ ファイルの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

Web コンテンツを含むファイルをディセーブルにし、削除して、セキュリティ アプライアンスのフラッシュ メモリからも削除するには、**revert webvpn content** コマンドを使用します。Web コンテンツを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、セキュリティ アプライアンスのフラッシュ メモリから ABCLogo という Web コンテンツ ファイルを削除するコマンドを示します。

```
hostname# revert webvpn webcontent abclogo
hostname
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn webcontent	現在セキュリティ アプライアンスのフラッシュ メモリに存在する Web コンテンツを表示します。

revocation-check

失効チェックの 1 つ以上の方法を設定するには、クリプト CA トラストポイント モードで **revocation-check** コマンドを使用します。セキュリティ アプライアンスでは、設定した順序で各方法が試みられます。2 つめおよび 3 つめの方法は、それよりも前の順序に設定されている方法でステータスが失効として検出されず、エラーが返された場合にのみ（サーバがダウンしているなど）試みられます。

クライアント証明書検証トラストポイントで、失効チェック方法を設定できます。また、レスポンダ証明書検証トラストポイントで、失効チェックなし（**revocation-check none**）を設定することもできます。**match certificate** コマンドのマニュアルに、設定手順の例が示されています。

デフォルトの失効チェック方法（*none*）に戻すには、このコマンドの **no** 形式を使用します。

revocation-check {[**crl**] [**none**] [**ocsp**]}

no revocation-check

構文の説明

crl	セキュリティ アプライアンスにおいて、失効チェック方法として CRL を使用する必要があることを指定します。
none	セキュリティ アプライアンスにおいて、すべての方法でエラーが返された場合でも証明書ステータスを有効であると解釈する必要があることを指定します。
ocsp	セキュリティ アプライアンスにおいて、失効チェック方法として OCSP を使用する必要があることを指定します。

デフォルト

デフォルト値は *none* です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。次のように各コマンドが置き換えられました。 • **crl optional** は **revocation-check crl none** に置き換えられました。 • **crl required** は **revocation-check crl** に置き換えられました。 • **crl nocheck** は **revocation-check none** に置き換えられました。

使用上のガイドライン

OCSP 応答の署名者は、通常、OCSP サーバ（レスポンダ）証明書です。デバイスは、応答を受信した後、レスポンダ証明書の検証を試みます。

通常、CA は、セキュリティが侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は、失効ステータス チェックが必要ないことを示す ocsp-no-check 拡張をレスポンダ証明書に組み込みます。ただし、この拡張がない場合、デバイスはこの **revocation-check** コマンドでトラストポイントに設定した失効チェック方法を使用して証明書の失効ステータスのチェックを試みます。ocsp-no-check 拡張がない場合は、OCSP レスポンダ証明書は検証可能である必要があります。検証可能でないと、*none* オプションを使用してステータス チェックを無視するように設定していない限り OCSP 失効チェックに失敗するためです。

例

次に、newtrust というトラストポイントに、失効チェック方法を OCSP、CRL の順で設定する例を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp crl
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバを指定します。

rewrite

WebVPN 接続上で、特定のアプリケーションまたはトラフィック タイプのコンテンツのリライトをディセーブルにするには、webvpn モードで **rewrite** コマンドを使用します。リライト ルールを削除するには、ルールを一意に識別するルール番号を指定して、このコマンドの **no** 形式を使用します。すべてのリライト ルールを削除するには、このコマンドの **no** 形式をルール番号を指定せずに使用します。

デフォルトで、セキュリティ アプライアンスでは、すべての WebVPN トラフィックがリライト（変換）されます。

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

構文の説明

disable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをディセーブルにするルールとして定義します。コンテンツのリライトをディセーブルにすると、トラフィックはセキュリティ アプライアンスを通過しません。
enable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをイネーブルにするルールとして定義します。
integer	設定されているすべてのルール内でのルールの順序を設定します。指定できる範囲は 1 ～ 65534 です。
name	（任意）ルールを適用するアプリケーションまたはリソースの名前を指定します。
order	セキュリティ アプライアンスがルールを適用する順序を定義します。
resource-mask	ルールのアプリケーションまたはリソースを指定します。
resource name	（任意）ルールを適用するアプリケーションまたはリソースを指定します。最大 128 バイトです。
string	照合するアプリケーションまたはリソースの名前を指定します。正規表現を使用できます。次のワイルドカードを使用できます。 照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ?：任意の 1 文字に一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 300 バイトです。

デフォルト

デフォルトでは、すべてをリライトします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、WebVPN 接続経由で正しくレンダリングされるように、アプリケーションのコンテンツがリライトされます。外部パブリック Web サイトなどの一部のアプリケーションでは、この処理は必要ありません。これらのアプリケーションでは、コンテンツ リライトをオフにできます。

disable オプションを指定して rewrite コマンドを使用することによって、コンテンツ リライトを選択的にオフにし、ユーザがセキュリティ アプライアンスを経由せずに直接特定のサイトをブラウズ可能にできます。これは、IPSec VPN 接続におけるスプリット トンネリングに似ています。

このコマンドは複数回使用できます。セキュリティ アプライアンスでは、順序番号に従ってリライト ルールが検索され、一致する最初のルールが適用されるため、エントリの設定順序は重要です。

例

次に、cisco.com ドメインの URL に対するコンテンツ リライトをオフにする順序番号 1 のリライト ルールを設定する例を示します。

```
hostname(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。

re-xauth

IPSec ユーザに対して IKE キー再生成時に再認証を要求するには、グループ ポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを発行します。IKE キー再生成時にユーザの再認証をディセーブルにするには、**re-xauth disable** コマンドを使用します。

実行コンフィギュレーションから re-xauth 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、他のグループ ポリシーから IKE キー再生成時の再認証についての値が継承されます。

re-xauth {**enable** [**extended**] | **disable**}

no re-xauth

構文の説明

disable	IKE キー再生成時の再認証をディセーブルにします。
enable	IKE キー再生成時の再認証をイネーブルにします。
extended	認証クレデンシャルを再入力可能な時間を、設定されている SA の最大ライフタイムまで延長します。

デフォルト

IKE キー再生成時の再認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0.4	**extended** キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IKE キー再生成時の再認証は、IPSec 接続に対してのみ適用されます。

IKE キー再生成時の再認証をイネーブルにすると、セキュリティ アプライアンスでは、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

ユーザは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。ユーザに対して、設定されている SA の最大ライフタイムまで認証クレデンシャルの再入力を許可するには、**extended** キーワードを使用します。

設定されているキー再生成間隔をチェックするには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータの KB 単位のライフタイムを表示します。

（注）　接続の他方の終端にユーザが存在しない場合、再認証は失敗します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、キー再生成時の再認証をイネーブルにする例を示します。

```
hostname(config) #group-policy FirstGroup attributes
hostname(config-group-policy)# re-xauth enable
```

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

rip send version {[**1**] [**2**]}

no rip send version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 パケットを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル RIP 送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {[**1**] [**2**]}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip authentication mode

RIP バージョン 2 パケットで使用される認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication mode** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

rip authentication mode {**text** | **md5**}

no rip authentication mode

構文の説明

md5	RIP メッセージ認証に MD5 を使用します。
text	RIP メッセージ認証にクリア テキストを使用します（非推奨）。

デフォルト

デフォルトで、クリア テキスト認証が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication key	RIP バージョン 2 認証をイネーブルにして、認証キーを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip authentication key

RIP バージョン 2 パケットの認証をイネーブルにして、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication key** コマンドを使用します。RIP バージョン 2 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

rip authentication key *key* **key_id** *key_id*

no rip authentication key

構文の説明

key	RIP 更新を認証するためのキー。このキーには、最大 16 文字を含めることができます。
key_id	キー ID 値。有効な値の範囲は 1 ～ 255 です。

デフォルト

RIP 認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。ネイバー認証をイネーブルにする場合は、*key* 引数および *key_id* 引数が、RIP バージョン 2 更新を提供するネイバー デバイスによって使用されているものと同じである必要があります。*key* は、最大 16 文字のテキスト ストリングです。

インターフェイス上で **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication mode	RIP バージョン 2 パケットで使用される認証のタイプを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

version {[**1**] [**2**]}

no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

rip send version {[**1**] [**2**]}

no rip send version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 パケットを送信します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル RIP 送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、セキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0:	（任意）非着脱式内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）着脱式外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）取り外しできない内蔵フラッシュを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）削除するディレクトリの絶対または相対パス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ディレクトリが空でない場合、**rmdir** コマンドは失敗します。

例

次の例は、「test」という名前の既存のディレクトリを削除する方法を示しています。

```
hostname# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイル システムに関する情報を表示します。

route

指定したインターフェイスにスタティック ルートまたはデフォルト ルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定したインターフェイスからルートを削除するには、このコマンドの **no** 形式を使用します。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

構文の説明

gateway_ip	ゲートウェイ ルータの IP アドレス（このルートのネクストホップ アドレス）を指定します。 **（注）** トランスペアレント モードでは、*gateway_ip* 引数は省略可能です。
interface_name	トラフィックがルーティングされる内部または外部ネットワーク インターフェイス名。
ip_address	内部または外部ネットワーク IP アドレス。
metric	（任意）このルートのアドミニストレーティブ ディスタンス。有効値の範囲は、1 ～ 255 です。デフォルト値は、1 です
netmask	*ip_address* に適用するネットワーク マスクを指定します。
track *number*	（任意）このルートにトラッキング エントリを関連付けます。有効な値は、1 ～ 500 です。 **（注）** **track** オプションは、シングル、ルーテッド モードでのみ使用できます。
tunneled	ルートを、VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

metric のデフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	**track** *number* の値が追加されました。

使用上のガイドライン

インターフェイスに対してデフォルト ルートまたはスタティック ルートを入力するには、**route** コマンドを使用します。デフォルト ルートを入力するには、*ip_address* および *netmask* を **0.0.0.0** または短縮形の **0** に設定します。**route** コマンドを使用して入力されたすべてのルートは、コンフィギュレーションの保存時に保存されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

tunneled オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

スタティック ルートは、任意のインターフェイスで、ルータの外部に接続されているネットワークにアクセスする場合に作成します。たとえば、セキュリティ アプライアンスはこのスタティック **route** コマンドを使用して、192.168.42.0 ネットワーク宛てのすべてのパケットを、192.168.1.5 ルータ経由で送信します。

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、セキュリティ アプライアンスは、ルート テーブルに CONNECT ルートを作成します。このエントリは、**clear route** コマンドや **clear configure route** コマンドを使用しても削除されません。

route コマンドでセキュリティ アプライアンス上のいずれかのインターフェイスの IP アドレスが使用されている場合、セキュリティ アプライアンスでは、ゲートウェイ IP アドレスではなく、パケット内の宛先 IP アドレスの ARP 解決が試みられます。

例

次に、外部インターフェイスに対して、1 つのデフォルト **route** コマンドを指定する例を示します。

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

次に、ネットワークへのアクセスを提供するスタティック **route** コマンドを追加する例を示します。

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

次に、SLA 動作を使用して、外部インターフェイスに対して、10.1.1.1 ゲートウェイへのデフォルト ルートをインストールする例を示します。SLA 動作では、このゲートウェイの可用性がモニタされます。SLA 動作に失敗した場合は、dmz インターフェイスのバックアップ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
```

```
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
hostname(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

route-map

ルーティング プロトコル間でルートを再配布する条件を定義するには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

構文の説明

deny	（任意）ルート マップで一致基準が満たされると、ルートが再配布されないことを指定します。
map_tag	ルート マップ タグの最大 57 文字のテキスト。
permit	（任意）このルート マップで一致基準が満たされると、設定アクションに従ってルートが再配布されることを指定します。
seq_num	（任意）ルート マップ シーケンス番号。有効な値は、0 ～ 65535 です。同じ名前ですでに設定されているルート マップのリスト内で新しいルート マップが配置される位置を示します。

デフォルト

デフォルトの設定は次のとおりです。

- **permit**
- *seq_num* を指定しない場合は、最初のルート マップに 10 の *seq_num* が割り当てられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

route-map コマンドを使用すると、ルートを再配布できます。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドでは、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件が定義されます。各 **route-map** コマンドには **match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは、任意の順序で入力できます。**set** コマンドによって指定された設定アクションに従ってルートが再配布されるためには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルーティング プロセス間でルートを再配布する方法を詳細に制御する必要がある場合にルート マップを使用します。宛先ルーティング プロトコルは、**router ospf** グローバル コンフィギュレーション コマンドを使用して指定します。送信元ルーティング プロトコルは、**redistribute** ルータ コンフィギュレーション コマンドを使用して指定します。

ルート マップに従ってルートを再配布する場合、複数の基準を使用してルート マップを構成できます。**route-map** コマンドに関連する少なくとも 1 つの match 句に一致しないルートは無視されます。発信ルート マップではルートはアドバタイズされず、着信ルート マップではルートは受け入れられません。一部のデータのみを変更するには、明示的な一致を指定した別のルート マップ セクションを設定する必要があります。

seq_number 引数の内容は次のとおりです。

1. 特定のタグにおいて、そのタグを指定したエントリを定義しない場合、*seq_number* 引数が 10 に設定されたエントリが作成されます。
2. 特定のタグにおいて、そのタグを指定したエントリを 1 つのみ定義した場合、そのエントリは後続の **route-map** コマンドのデフォルト エントリとなります。このエントリの *seq_number* 引数は変更されません。
3. 特定のタグにおいて、そのタグを指定したエントリを複数定義した場合は、*seq_number* 引数が必要であることを示すエラー メッセージが表示されます。

no route-map *map-tag* コマンドが（*seq-num* 引数なしで）指定されている場合、ルート マップ全体（同じ *map-tag* テキストを持つすべての **route-map** エントリ）が削除されます。

一致基準が満たされなかった場合、**permit** キーワードが指定されていると、同じ *map_tag* を持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。

例

次に、OSPF ルーティングでルート マップを設定する例を示します。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
router ospf	OSPF ルーティング プロセスを開始および設定します。

コマンド	説明
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。
show running-config route-map	ルート マップ コンフィギュレーションの情報を表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モードで **router-id** コマンドを使用します。以前のルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *addr*

no router-id [*addr*]

構文の説明

addr	IP アドレス形式でのルータ ID。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	このコマンドの処理順序が変更されました。このコマンドは、OSPF コンフィギュレーションでは、**network** コマンドよりも先に処理されるようになりました。

使用上のガイドライン

セキュリティ アプライアンスでは、OSPF コンフィギュレーションにおいて、デフォルトで、**network** コマンドによって指定されているインターフェイス上の最上位の IP アドレスが使用されます。最上位の IP アドレスがプライベート アドレスである場合、そのアドレスは hello パケットおよびデータベース定義で送信されます。特定のルータ ID を使用するには、**router-id** コマンドを使用して、ルータ ID としてグローバル アドレスを指定します。

ルータ ID は、OSPF ルーティング ドメイン内で一意である必要があります。同じ OSPF ドメイン内の 2 つのルータが同じルータ ID を使用している場合、ルーティングが正しく動作しない可能性があります。

OSPF コンフィギュレーションでは、**network** コマンドを入力する前に **router-id** コマンドを入力する必要があります。これにより、セキュリティ アプライアンスによって生成されるデフォルトのルータ ID との競合を回避できます。競合がある場合は、次のメッセージが表示されます。

```
ERROR: router-id addr in use by ospf process pid
```

競合する ID を入力するには、競合の原因となっている IP アドレスを含む **network** コマンドを削除し、**router-id** コマンドを入力して、**network** コマンドを再入力します。

例

次に、ルータ ID を 192.168.1.1 に設定する例を示します。

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

router eigrp

EIGRP ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router eigrp** コマンドを使用します。EIGRP ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

router eigrp *as-number*

no router eigrp *as-number*

構文の説明

as-number	他の EIGRP ルータへのルートを識別する自律システム番号。ルーティング情報のタギングにも使用されます。有効な値は 1 ～ 65535 です。

デフォルト

EIGRP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

router eigrp コマンドは、EIGRP ルーティング プロセスを作成するか、または既存の EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。セキュリティ アプライアンスでは、単一の EIGRP ルーティング プロセスのみを作成できます。

次のルータ コンフィギュレーション モード コマンドを使用して、EIGRP ルーティング プロセスを設定します。

- **auto-summary**：自動ルート集約をイネーブルまたはディセーブルにします。
- **default-information**：デフォルト ルート情報の送受信をイネーブルまたはディセーブルにします。
- **default-metric**：EIGRP ルーティング プロセスに再配布されるルートのデフォルトのメトリックを定義します。
- **distance eigrp**：内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定します。
- **distribute-list**：ルーティング更新で送受信されるネットワークをフィルタリングします。
- **eigrp log-neighbor-changes**：ネイバー ステートの変更のロギングをイネーブルまたはディセーブルにします。

- **eigrp log-neighbor-warnings**：ネイバー警告メッセージのロギングをイネーブルまたはディセーブルにします。
- **eigrp router-id**：固定ルータ ID を作成します。
- **eigrp stub**：セキュリティ アプライアンスでスタブ EIGRP ルーティングを設定します。
- **neighbor**：EIGRP ネイバーをスタティックに定義します。
- **network**：EIGRP ルーティング プロセスに参加するネットワークを設定します。
- **passive-interface**：パッシブ インターフェイスとして動作するインターフェイスを設定します。
- **redistribute**：他のルーティング プロセスから EIGRP にルートを再配布します。

次のインターフェイス コンフィギュレーション モード コマンドを使用して、インターフェイス固有の EIGRP パラメータを設定します。

- **authentication key eigrp**：EIGRP メッセージ認証で使用される認証キーを定義します。
- **authentication mode eigrp**：EIGRP メッセージ認証で使用される認証アルゴリズムを定義します。
- **delay**：インターフェイスの遅延メトリックを設定します。
- **hello-interval eigrp**：EIGRP の hello パケットがインターフェイスから送信される間隔を変更します。
- **hold-time eigrp**：セキュリティ アプライアンスによってアドバタイズされるホールド タイムを変更します。
- **split-horizon eigrp**：インターフェイスで EIGRP スプリット ホライズンをイネーブルまたはディセーブルにします。
- **summary-address eigrp**：サマリー アドレスを手動で定義します。

例

次に、自律システム番号 100 が付けられた EIGRP ルーティング プロセスのコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

router ospf

OSPF ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router ospf** コマンドを使用します。OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

router ospf *pid*

no router ospf *pid*

構文の説明

pid	OSPF ルーティング プロセスの内部的に使用される ID パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータの OSPF プロセスの ID と一致する必要はありません。

デフォルト

OSPF ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

router ospf コマンドは、セキュリティ アプライアンス上で実行される OSPF ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、ルータ コンフィギュレーション モードであることを示す (config-router)# コマンド プロンプトが表示されます。

no router ospf コマンドを使用する場合は、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no router ospf** コマンドは、*pid* によって指定された OSPF ルーティング プロセスを終了します。*pid* は、セキュリティ アプライアンスにおいてローカルに割り当てます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、次の OSPF 固有のコマンドとともに、OSPF ルーティング プロセスを設定するために使用されます。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：集約ルートのコスト計算に使用される方法を RFC 1583 に従った方法に戻します。
- **default-information originate**：OSPF ルーティング ドメインへのデフォルト外部ルートを生成します。

- **distance**：ルート タイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを定義します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合の syslog メッセージの送信を抑制します。
- **log-adj-changes**：OSPF ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
- **neighbor**：隣接ルータを指定します。VPN トンネル経由での隣接関係の確立を許可するために使用します。
- **network**：OSPF が実行されるインターフェイス、およびそれらのインターフェイスのエリア ID を定義します。
- **redistribute**：指定されたパラメータに従って、ルーティング ドメイン間でのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timers lsa-group-pacing**：OSPF LSA グループ ペーシング タイマー（LSA のグループがリフレッシュされる間隔または最大エージング期間に達するまでの間隔）。
- **timers spf**：SPF 計算の変更を受信するまでの遅延。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router ospf 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドをクリアします。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。

router rip

RIP ルーティング プロセスを開始して、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router rip** コマンドを使用します。RIP ルーティング プロセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

router rip

no router rip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

RIP ルーティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

router rip コマンドは、セキュリティ アプライアンス上の RIP ルーティング プロセスを設定するためのグローバル コンフィギュレーション コマンドです。セキュリティ アプライアンスでは、1 つの RIP プロセスのみを設定できます。**no router rip** コマンドは、RIP ルーティング プロセスを終了し、そのプロセスのすべてのルータ コンフィギュレーションを削除します。

router rip コマンドを入力すると、コマンド プロンプトが、ルータ コンフィギュレーション モードであることを示す `hostname(config-router)#` に変更されます。

router rip コマンドは、次のルータ コンフィギュレーション コマンドとともに、RIP ルーティング プロセスを設定するために使用されます。

- **auto-summary**：ルートの自動集約をイネーブルまたはディセーブルにします。
- **default-information originate**：デフォルト ルートを配布します。
- **distribute-list in**：着信ルーティング更新のネットワークをフィルタリングします。
- **distribute-list out**：発信ルーティング更新のネットワークをフィルタリングします。
- **network**：ルーティング プロセスでインターフェイスを追加または削除します。
- **passive-interface**：特定のインターフェイスをパッシブ モードに設定します。
- **redistribute**：他のルーティング プロセスから RIP ルーティング プロセスにルートを再配布します。

- **version**：セキュリティ アプライアンスで使用される RIP プロトコル バージョンを設定します。

また、次のコマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスごとの RIP プロパティを設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 によって使用される認証のタイプを設定します。
- **rip send version**：インターフェイスから更新を送信するために使用する RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。
- **rip receive version**：インターフェイスで受け入れる RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。

トランスペアレント モードでは、RIP はサポートされていません。デフォルトで、セキュリティ アプライアンスは、すべての RIP ブロードキャスト パケットおよびマルチキャスト パケットを拒否します。これらの RIP メッセージが、トランスペアレント モードで動作するセキュリティ アプライアンスを通過できるようにするには、このトラフィックを許可するアクセス リスト エントリを定義する必要があります。たとえば、RIP バージョン 2 トラフィックがセキュリティ アプライアンスを通過することを許可するには、`access-list myriplist extended permit ip any host 224.0.0.9` のようなアクセス リスト エントリを作成します。RIP バージョン 1 ブロードキャストを許可するには、`access-list myriplist extended permit udp any any eq rip` のようなアクセス リスト エントリを作成します。**access-group** コマンドを使用して、これらのアクセス リスト エントリを適切なインターフェイスに適用します。

セキュリティ アプライアンスでは、RIP ルーティングと OSPF ルーティングの両方を同時にイネーブルにできます。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
clear configure router rip	実行コンフィギュレーションから RIP ルータ コマンドをクリアします。
show running-config router rip	実行コンフィギュレーション内の RIP ルータ コマンドを表示します。

rtp-conformance

ピンホールを通過する RTP パケットが H.323 および SIP プロトコルに準拠しているかどうかをチェックするには、パラメータ コンフィギュレーション モードで **rtp-conformance** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

構文の説明

enforce-payloadtype	シグナリング交換に基づいて、ペイロード タイプをオーディオまたはビデオであると指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ピンホールを通過する RTP パケットが H.323 コールのプロトコルに準拠しているかどうかをチェックする例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# rtp-conformance
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
debug rtp	H.323 および SIP インスペクションに関連する RTP パケットのデバッグ情報およびエラー メッセージを表示します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。