Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンドおよび ASASM 用 IOS コマンド

Cisco Systems, Inc.
http://www.cisco.com/jp

Cisco は世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices をご覧ください。

Text Part Number: なし、オンライン専用

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンドおよびASASM 用 IOS コマンド

パート 1

T ～ Z コマンド

table-map through title

table-map

IP ルーティングテーブルが BGP で学習されたルートで更新された場合にメトリックおよびタグ値を変更するには、アドレス ファミリ コンフィギュレーション モードで **table-map** 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、コマンドの **no** 形式を使用します。

table-map *map-name* [**filter**]

no table-map *map-name* [**filter**]

構文の説明

map_name	BGP ルーティングテーブル（RIB）に追加する内容を制御する必要があるルートマップの名前。
filter	（オプション）ルートマップが BGP ルートのメトリックだけでなく、そのルートが RIB にダウンロードされるかどうかも制御することを指定します。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

テーブルマップで、BGP ルーティングテーブル内で更新されるルートのメトリックおよびタグ値を設定するルートマップを参照するか、またはルートを RIB にダウンロードするかどうかを制御します。

table-map コマンドに、

- **filter** キーワードが含まれていない場合、参照されるルートマップは、ルートが RIB にインストール（ダウンロード）される前に、ルートの特定のプロパティを設定するために使用されます。ルートは、ルート マップで許可されているか拒否されているかにかかわらず、常にダウンロードされます。
- **filter** キーワードが含まれている場合、参照されるルートマップも BGP ルートが RIB にダウンロードされるかどうかを制御します。BGP ルートは、ルート マップで拒否されている場合、RIB にダウンロードされません。

テーブルマップが参照するルートマップで match 句を使用すると、IP アクセスリスト、自律システム（AS）パス、およびネクストホップに基づいてルートを照合できます。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、ASA ソフトウェアは、BGP で学習されたルートのタグ値を自動的に計算し、IP ルーティング テーブルを更新するように設定されています。

```
ciscoasa(config)# route-map tag
ciscoasa(config-route-map)# match as path 10
ciscoasa(config-route-map)# set automatic-tag

ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# table-map tag
```

関連コマンド

コマンド	説明
address-family	アドレス ファミリ コンフィギュレーション モードを開始します。
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条件を定義します。

tcp-inspection

DNS over TCP インスペクション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 **tcp-inspection** コマンドを使用します。プロトコルの強制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。

tcp-inspection

no tcp-inspection

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

DNS over TCP インスペクション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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマン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 DNS インスペクション ポリシー マップに追加して、DNS/TCP ポート 53 トラフィックをインスペクションに含めます。このコマンドを使用しなければ、UDP/53 DNS トラフィックのみが検査されます。DNS/TCP ポート 53 トラフィックが、DNS インスペクションを適用するクラスの一部であることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれています。

例

次に、DNS インスペクション ポリシー マップで DNS over TCP インスペクションをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tcp-inspection
```

関連コマンド

コマンド	説明
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション 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。

tcp-map

一連の TCP 正規化アクションを定義するには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP 正規化機能によって、異常なパケットを識別する基準を指定できます。ASA は、異常なパケットが検出されるとそれらをドロップします。TCP 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。

tcp-map *map_name*

no tcp-map *map_name*

構文の説明

map_name	TCP マップ名を指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)/8.0(4)	**invalid-ack**、**seq-past-window**、および **synack-data** サブコマンドが追加されました。

使用上のガイドライン

この機能は モジュラ ポリシー フレームワークを使用します。最初に、**tcp-map** コマンドを使用して実行する TCP 正規化アクションを定義します。**tcp-map** コマンドによって、tcp マップ コンフィギュレーション モードが開始されます。このモードで、1 つ以上のコマンドを入力して、TCP 正規化アクションを定義できます。その後、**class-map** コマンドを使用して、TCP マップを適用するトラフィックを定義します。**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection advanced-options** コマンドを入力して TCP マップを参照します。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

次のコマンドは、tcp マップ コンフィギュレーション モードで使用可能です。

check-retransmission	再送信データのチェックをイネーブルまたはディセーブルにします。
checksum-verification	チェックサムの検証をイネーブルまたはディセーブルにします。
exceed-mss	ピアによって設定された MSS を超えるパケットを許可またはドロップします。
invalid-ack	無効な ACK を含むパケットに対するアクションを設定します。
queue-limit	TCP 接続のキューに入れることができる順序が不正なパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズ ASA でのみ使用可能です。PIX 500 シリーズ ASA ではキュー制限は 3 で、この値は変更できません。
reserved-bits	ASA に予約済みフラグ ポリシーを設定します。
seq-past-window	パストウィンドウ シーケンス番号を含むパケットに対するアクションを設定します。つまり、受信した TCP パケットのシーケンス番号が、TCP 受信ウィンドウの右端より大きい場合です。
synack-data	データを含む TCP SYNACK パケットに対するアクションを設定します。
syn-data	データを持つ SYN パケットを許可またはドロップします。
tcp-options	TCP ヘッダーの TCP オプション フィールドの内容に基づいて、パケットのアクションを設定します。
ttl-evasion-protection	ASA によって提供された TTL 回避保護をイネーブルまたはディセーブルにします。
urgent-flag	ASA を通じて URG ポインタを許可またはクリアします。
window-variation	予期せずウィンドウ サイズが変更された接続をドロップします。

例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow

ciscoasa(config-tcp-map)# class-map urg-class
ciscoasa(config-cmap)# match port tcp range ftp-data telnet

ciscoasa(config-cmap)# policy-map pmap
ciscoasa(config-pmap)# class urg-class
ciscoasa(config-pmap-c)# set connection advanced-options tmap

ciscoasa(config-pmap-c)# service-policy pmap global
```

関連コマンド

コマンド	説明
class（ポリシーマップ）	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。
clear configure tcp-map	TCP マップのコンフィギュレーションをクリアします。
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。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。

tcp-options

TCP ヘッダーの TCP オプションを許可またはクリアするには、TCP マップ コンフィギュレーション モードで **tcp-options** 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。

tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

no tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

構文の説明

アクション	オプションのために実行するアクションです。アクションは次のとおりです。 • **allow** [**multiple**]：オプションを含むパケットを許可します。9.6(2) 以降では、**allow** はこのタイプの単一のオプションを含むパケットを許可することを意味します。これは、すべての名前付きオプションのデフォルトです。オプションのインスタンスが複数含まれていてもパケットを許可する場合は、**multiple** キーワードを追加します。**multiple** キーワードは、**range** と一緒には使用できません。 • **maximum** *limit*：**mss** 専用。最大セグメント サイズを、示された制限（68 ～ 65535）に設定します。デフォルトの TCP MSS は、**sysopt connection tcpmss** コマンドで定義されます。 • **clear**：このタイプのオプションをヘッダーから削除して、パケットを許可します。これは、**range** キーワードで設定できるすべての番号付きオプションのデフォルトです。タイムスタンプ オプションを消去すると、PAWS と RTT がディセーブルになります。 • **drop**：このオプションを含むパケットをドロップします。このアクションは、**md5** および **range** だけで利用可能です。
md5	MD5 オプションのアクションを設定します。
mss	最大セグメント サイズ オプションのアクションを設定します。
range *lower upper*	範囲の下限および上限内の番号付きオプションのアクションで設定します。単一の番号付きオプションのアクションを設定するには、範囲の下限と上限に同じ数値を入力します。 （9.6(2) 以降）有効範囲は、6 ～ 7、9 ～ 18、および 20 ～ 255 以内です。 （9.6(1) 以降）有効範囲は、6 ～ 7 および 9 ～ 255 以内です。
selective-ack	選択的確認応答メカニズム（SACK）オプションのアクションを設定します。
timestamp	タイムスタンプ オプションのアクションを設定します。タイムスタンプ オプションをクリアすると、PAWS と RTT がディセーブルになります。
window-scale	ウィンドウ スケール メカニズム オプションのアクションを設定します。

デフォルト

(9.6(1) 以降)デフォルトでは、すべての名前付きオプションを許可し、オプション 6 ～ 7 および 9 ～ 255 をクリアします。

(9.6(2) 以降)デフォルトでは、名前付きオプションのそれぞれの 1 つのインスタンスを許可し、指定された名前付きオプションが複数あるパケットをドロップし、オプション 6 ～ 7、9 ～ 18、および 20 ～ 155 をクリアします。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(2)	名前付きオプションのデフォルト処理は、指定されたタイプのオプションを 1 つ含む場合はパケットを許可し、そのタイプのオプションが複数ある場合はパケットをドロップするように変更されました。また、**md5**、**mss**、**allow multiple**、および **mss maximum** キーワードが追加されました。MD5 オプションのデフォルトは、クリアから許可に変更されました。

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。TCP マップ コンフィギュレーション モードで **tcp-options** コマンドを使用して、さまざまな TCP オプションを処理する方法を定義します。

例

次に、6 ～ 7 および 9 ～ 255 の範囲内の TCP オプションを持つすべてのパケットをドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# tcp-options range 6 7 drop
ciscoasa(config-tcp-map)# tcp-options range 9 18 drop
ciscoasa(config-tcp-map)# tcp-options range 20 255 drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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。

telnet

インターフェイスへの Telnet アクセスを許可するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。Telnet アクセスを削除するには、このコマンドの **no** 形式を使用します。

telnet {*ipv4_address mask* | *ipv6_address/prefix*} *interface_name*

no telnet {*ipv4_address mask* | *ipv6_address/prefix*} *interface_name*

構文の説明

interface_name	Telnet を許可するインターフェイスの名前を指定します。VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスで Telnet をイネーブルにできません。物理または仮想インターフェイスを指定できます。
ipv4_address mask	ASA への Telnet が認可されているホストまたはネットワークの IPv4 アドレス、およびサブネット マスクを指定します。
ipv6_address/prefix	ASA への Telnet が認可されている IPv6 アドレスおよびプレフィックスを指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(2)、9.1(2)	デフォルト パスワードの「cisco」は削除されました。**password** コマンドを使用して能動的にログイン パスワードを設定する必要があります。
9.9.(2)	仮想インターフェイスが指定可能になりました。

使用上のガイドライン

telnet コマンドを使用すると、どのホストが Telnet を使用して ASA の CLI にアクセスできるかを指定できます。すべてのインターフェイスで ASA への Telnet をイネーブルにすることができます。ただし、VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。また、BVI インターフェイスが指定されている場合、そのインターフェイスで **managenent-access** を設定する必要があります。

password コマンドを使用して、コンソールへの Telnet アクセスのパスワードを設定できます。**who** コマンドを使用して、現在、ASA コンソールにアクセス中の IP アドレスを表示できます。**kill** コマンドを使用すると、アクティブ Telnet コンソール セッションを終了できます。

aaa authentication telnet console コマンドを使用する場合は、Telnet コンソール アクセスを認証サーバで認証する必要があります。

例

次に、ホスト 192.168.1.3 と 192.168.1.4 に Telnet を介した ASA の CLI へのアクセスを許可する例を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストにアクセス権が付与されています。

```
ciscoasa(config)# telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.1.4 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.2.0 255.255.255.0 inside
ciscoasa(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

次に、Telnet コンソール ログイン セッションの例を示します（パスワードは、入力時に表示されません）。

```
ciscoasa# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
ciscoasa>
```

no telnet コマンドを使用して個々のエントリを、また、**clear configure telnet** コマンドを使用してすべての telnet コマンド ステートメントを削除できます。

```
ciscoasa(config)# no telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

ciscoasa(config)# clear configure telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	ASA への Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
telnet timeout	Telnet タイムアウトを設定します。
who	ASA 上のアクティブ Telnet 管理セッションを表示します。

telnet timeout

Telnet のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

telnet timeout *minutes*

no telnet timeout *minutes*

構文の説明

minutes	Telnet セッションがアイドルになってから、ASA がセッションを閉じるまでの分数。有効な値は、1 ～ 1440 分です。デフォルトは 5 分です。

デフォルト

デフォルトでは、Telnet セッションは、アイドル状態のまま 5 分経過すると ASA によって閉じられます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

telnet timeout コマンドを使用して、コンソール Telnet セッションが、ASA によってログオフされるまでアイドル状態を継続できる最長時間を設定できます。

例

次に、セッションの最大アイドル時間を変更する例を示します。

```
ciscoasa(config)# telnet timeout 10
ciscoasa(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	ASA への Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
telnet	ASA への Telnet アクセスをイネーブルにします。
who	ASA 上のアクティブ Telnet 管理セッションを表示します。

terminal interactive

CLI で **?** を入力したときに、現在の CLI セッションでヘルプを有効にするには、特権 EXEC モードで **terminal interactive** コマンドを使用します。CLI ヘルプ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。

terminal interactive

no terminal interactive

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

デフォルトでは、インタラクティブな CLI のヘルプは有効になっています。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

通常、ASA CLI で **?** を入力すると、コマンドのヘルプが表示されます。コマンド内にテキストとして **?** を入力できるようにするには（たとえば、URL の一部として **?** を含めるには）、**no terminal interactive** コマンドを使用してインタラクティブなヘルプをディセーブルにします。

例

次に、コンソールを非インタラクティブ モードにして、その後インタラクティブ モードにする例を示します。

```
ciscoasa# no terminal interactive
ciscoasa# terminal interactive
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal monitor

現在の CLI セッションで syslog メッセージの表示を許可するには、特権 EXEC モードで **terminal monitor** コマンドを使用します。syslog メッセージ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。

terminal {**monitor** | **no monitor**}

構文の説明

モニタ	現在の CLI セッションでの syslog メッセージの表示をイネーブルにします。
no monitor	現在の CLI セッションでの syslog メッセージの表示をディセーブルにします。

デフォルト

デフォルトでは、syslog メッセージはディセーブルです。このコマンドは、デフォルトではインタラクティブです。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、現在のセッションで syslog メッセージを表示する例およびディセーブルにする例を示します。

```
ciscoasa# terminal monitor
ciscoasa# terminal no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。

コマンド	説明
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal pager

Telnet セッションで「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

構文の説明

[**lines**] *lines*	「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。

デフォルト

デフォルトは 24 行です。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、現在の Telnet セッションのみを対象に、pager line 設定を変更します。ただし、ユーザ EXEC モードで **login** コマンドを入力するか、**enable** コマンドを入力して特権 EXEC モードを開始する場合にのみ、ASA は running-config から現在のセッションで pager 値を再開します。これは設計どおりです。

（注） ASA がユーザ プロンプトを再表示する前に、予期しない「--- More---」プロンプトが表示されます。これによって、**banner exec** コマンドの出力が抑制されることがあります。代わりに、**banner motd** コマンドまたは **banner login** コマンドを使用します。

新しいデフォルトの pager 設定をコンフィギュレーションに保存するには、次の手順を実行します。

1. **login** コマンドを入力してユーザ EXEC モードにアクセスするか、**enable** コマンドを入力して特権 EXEC モードにアクセスします。
2. **pager** コマンドを入力します。

管理コンテキストに Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次に、表示される行数を 20 に変更する例を示します。

```
ciscoasa# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---More---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal	Telnet セッションでの syslog メッセージの表示を許可します。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal width

コンソール セッションで情報を表示する幅を設定するには、グローバル コンフィギュレーション モードで **terminal width** コマンドを使用します。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。

terminal width *columns*

no terminal width *columns*

構文の説明

columns	端末の幅をカラム数で指定します。デフォルトは 80 です。指定できる範囲は 40 ～ 511 です。

デフォルト

デフォルトの表示幅は 80 カラムです。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、端末の表示幅を 100 カラムにする例を示します。

```
ciscoasa# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	端末回線パラメータを特権 EXEC モードで設定します。

test aaa-server

ASA が特定の AAA サーバでユーザを認証または認可できるかどうかを確認するには、特権 EXEC モードで **test aaa-server** コマンドを使用します。ASA 上の不正なコンフィギュレーションが原因で AAA サーバに到達できない場合があります。また、限定されたネットワーク コンフィギュレーションやサーバのダウンタイムなどの他の理由で AAA サーバに到達できないこともあります。

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*][**ad-agent**]}

構文の説明

ad-agent	AAA AD エージェント サーバへの接続をテストします。
authentication	AAA サーバの認証機能をテストします。
authorization	AAA サーバのレガシー VPN 認可機能をテストします。
host *ip_address*	サーバの IP アドレスを指定します。コマンドで IP アドレスを指定しないと、入力を求めるプロンプトが表示されます。
password *password*	ユーザ パスワードを指定します。コマンドでパスワードを指定しないと、入力を求めるプロンプトが表示されます。
server_tag	**aaa-server** コマンドで設定した AAA サーバ タグを指定します。
username *username*	AAA サーバの設定をテストするために使用するアカウントのユーザ名を指定します。ユーザ名が AAA サーバに存在することを確認してください。存在しないと、テストは失敗します。コマンドでユーザ名を指定しないと、入力を求めるプロンプトが表示されます。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
8.4(2)	**ad-agent** キーワードが追加されました。

使用上のガイドライン

test aaa-server コマンドでは、ASA が特定の AAA サーバを使用してユーザを認証できることと、ユーザを認可できる場合は、レガシー VPN 認可機能を確認できます。このコマンドを使用すると、認証または認可を試みる実際のユーザを持たない AAA サーバをテストできます。また、AAA 障害の原因が、AAA サーバ パラメータの設定ミス、AAA サーバへの接続問題、または ASA 上のその他のコンフィギュレーション エラーのいずれによるものかを特定するうえで役立ちます。

例

次に、ホスト 192.168.3.4 に srvgrp1 という RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、さらに認証ポートを 1650 に設定する例を示します。AAA サーバ パラメータのセットアップの後の **test aaa-server** コマンドによって、認証テストがサーバに到達できなかったことが示されます。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

次に、正常な結果となった **test aaa-server** コマンドの出力例を示します。

```
ciscoasa# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

関連コマンド

コマンド	説明
aaa authentication console	管理トラフィックの認証を設定します。
aaa authentication match	通過するトラフィックの認証を設定します。
aaa-server	AAA サーバ グループを作成します。
aaa-server host	AAA サーバをサーバ グループに追加します。

test aaa-server ad-agent

設定後に Active Directory エージェントのコンフィギュレーションをテストするには、AAA サーバ グループ コンフィギュレーション モードで **test aaa-server ad-agent** コマンドを使用します。

test aaa-server ad-agent

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ グループ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールに対して Active Directory エージェントを設定するには、**aaa-server** コマンドのサブモードである **ad-agent-mode** コマンドを入力します。**ad-agent-mode** コマンドを入力すると、AAA サーバ グループ コンフィギュレーション モードが開始します。

Active Directory エージェントの設定後、**test aaa-server ad-agent** コマンドを入力して、ASA に Active Directory エージェントへの機能接続があることを確認します。

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバのセキュリティ イベント ログ ファイルをモニタし、ユーザのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザ ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します。

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールに対して Active Directory エージェントを設定する際に **ad-agent-mode** をイネーブルにし、接続をテストする例を示します。

```
hostname(config)# aaa-server adagent protocol radius
hostname(config)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
hostname(config-aaa-server-host)# key mysecret
hostname(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
hostname(config-aaa-server-host)# test aaa-server ad-agent
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

test dynamic-access-policy attributes

dap 属性モードを開始するには、特権 EXEC モードで、**test dynamic-access-policy attributes** コマンドを入力します。これにより、ユーザ属性とエンドポイント属性の値ペアを指定できます。

dynamic-access-policy attributes

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

通常、ASA は AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。ASA は、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

この機能は、DAP レコードの作成を試みます。

例

次に、**attributes** コマンドの使用例を示します。

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
attributes	ユーザ属性値ペアを指定できる属性モードを開始します。
display	現在の属性リストを表示します。

test dynamic-access-policy execute

すでに設定されている DAP レコードをテストするには、特権 EXEC モードで test dynamic-access-policy execute を使用します。

test dynamic-access-policy execute

構文の説明

AAA attribute value	デバイスの DAP サブシステムは、各レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに、これらの値を参照します。 – [AAA Attribute]: AAA 属性を特定します。 – [Operation Value]: 属性を指定された値に対して =/!= として指定します。
endpoint attribute value	エンドポイント属性を指定します。 – [Endpoint ID]: エンドポイント属性 ID を入力します。 – [Name/Operation/Value]:

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(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

このコマンドでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。

test regex

正規表現をテストするには、特権 EXEC モードで **test regex** コマンドを使用します。

test regex *input_text regular_expression*

構文の説明

input_text	正規表現と一致させるテキストを指定します。
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、**regex** コマンド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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

test regex コマンドは、正規表現が一致すべきものと一致するかどうかをテストします。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

例

次に、正規表現に対して入力テキストをテストする例を示します。

```
ciscoasa# test regex farscape scape
INFO: Regular expression match succeeded.

ciscoasa# test regex farscape scaper

INFO: Regular expression match failed.
```

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	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。
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。
regex	正規表現を作成します。

test sso-server（廃止）

(注) このコマンドをサポートする最後のリリースは、バージョン 9.5(1) でした。

テスト用の認証要求で SSO サーバをテストするには、特権 EXEC モードで **test sso-server** コマンドを使用します。

test sso-server *server-name* **username** *user-name*

構文の説明

server-name	テストする SSO サーバの名前を指定します。
user-name	テストする SSO サーバのユーザの名前を指定します。

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
config-webvpn	• 対応	—	• 対応	—	—
config-webvpn-sso-saml	• 対応	—	• 対応	—	—
config-webvpn-sso-siteminder	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション モード	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

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。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、さらに、認証要求に応答しているかどうかをテストします。

server-name 引数で指定された SSO サーバが見つからない場合は、次のエラーが表示されます。

```
ERROR: sso-server server-name does not exist
```

SSO サーバが見つかったが、*user-name* 引数で指定されたユーザが見つからない場合は、認証は拒否されます。

認証では、ASA は SSO サーバへの WebVPN ユーザのプロキシとして動作します。ASA は現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。このコマンドは SSO サーバの両タイプに適用されます。

例

次に、特権 EXEC モードを開始し、ユーザ名 Anyuser を使用して SSO サーバ my-sso-server をテストし、正常な結果を得た例を示します。

```
ciscoasa# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
ciscoasa#
```

次に、同じサーバだが、ユーザ Anotheruser でテストし、認識されず、認証が失敗した例を示します。

```
ciscoasa# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
ciscoasa#
```

関連コマンド

コマンド	説明
max-retry-attempts	ASA 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。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
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。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

text-color

ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定するには、webvpn モードで **text-color** コマンドを使用します。テキストの色をコンフィギュレーションから削除して、デフォルト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。

text-color [*black* | *white* | *auto*]

no text-color

構文の説明

auto	secondary-color コマンドの設定に基づいて黒または白を選択します。つまり、2 番めの色が黒の場合、この値は白となります。
black	タイトルバーのテキストのデフォルト色は白です。
white	色を黒に変更できます。

デフォルト

タイトルバーのテキストのデフォルト色は白です。

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	トランスペアレント	シングル	コンテキスト	システム
config-webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、タイトルバーのテキストの色を黒に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# text-color black
```

関連コマンド

コマンド	説明
secondary-text-color	WebVPN ログイン ページ、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定します。

tftp blocksize

TFTP のブロックサイズ値を設定するには、グローバル コンフィギュレーション モードで **tftp blocksize** コマンドを使用します。ブロックサイズの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。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

tftp blocksize *number*

no tftp blocksize

構文の説明

number	設定するブロックサイズの値を指定します。この値は、513 ～ 8192 オクテットの範囲で指定できます。ブロックサイズの新しいデフォルト設定は、1456 オクテットです。

デフォルト

新しいデフォルト値は 1456 オクテットです。サーバがこのネゴシエーションをサポートしていない場合、古いデフォルト値（512 オクテットサイズ）が優先されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 可

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが追加されました。

使用上のガイドライン

tftp blocksize コマンドを使用すると、より大きなブロックサイズを設定して tftp ファイルの転送速度を向上させることができます。この設定可能なブロックサイズ値オプションは、tftp の読み取りおよび書き込みリクエストに追加され、確認のために tftp サーバに送信されます。オプションの確認応答（OACK）を受信すると、設定したブロックサイズ値でファイル転送が開始されます。新しいデフォルトのブロックサイズは 1456 オクテットです。このコマンドの **no** 形式を指定すると、ブロックサイズが古いデフォルト値（512 オクテット）にリセットされます。

show running-configuration コマンドによって、設定したブロックサイズ値（デフォルト値を除く）が表示されます。

例

次に、TFTP ブロックサイズ値を指定する方法の例を示します。

```
ciscoasa(config)# tftp blocksize 2048
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show running-config tftp blocksize	設定したブロックサイズの値(デフォルト値を除く)を表示します。

tftp-server

configure net コマンドまたは **write net** コマンドで使用するデフォルトの TFTP サーバとパスおよびファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

構文の説明

filename	パスとファイル名を指定します。
interface_name	ゲートウェイ インターフェイス名を指定します。最高のセキュリティ インターフェイス以外のインターフェイスを指定した場合は、そのインターフェイスがセキュアではないことを示す警告メッセージが表示されます。
サーバ	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 アドレスまたは IPv6 アドレスを入力できます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	現在ではゲートウェイ インターフェイスが必要です。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** コマンドと **write net** コマンドの入力が容易になります。**configure net** コマンドまたは **write net** コマンドを入力するときに、**tftp-server** コマンドで指定した TFTP サーバを継承するか、または独自の値を指定できます。また、**tftp-server** コマンドのパスをそのまま継承したり、**tftp-server** コマンド値の末尾にパスとファイル名を追加したり、**tftp-server** コマンド値を上書きすることもできます。

ASA がサポートする **tftp-server** コマンドは 1 つだけです。

例

次に、TFTP サーバを指定し、その後、/temp/config/test_config ディレクトリからコンフィギュレーションを読み込む例を示します。

```
ciscoasa(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
ciscoasa(config)# configure net
```

関連コマンド

コマンド	説明
configure net	指定した TFTP サーバとパスからコンフィギュレーションをロードします。
show running-config tftp-server	デフォルトの TFTP サーバ アドレスとコンフィギュレーション ファイルのディレクトリを表示します。

tftp-server address（廃止）

クラスタ内の TFTP サーバを指定するには、電話プロキシ コンフィギュレーション モードで **tftp-server address** コマンドを使用します。電話プロキシ コンフィギュレーションから TFTP サーバを削除するには、このコマンドの **no** 形式を使用します。

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

構文の説明

ip_address	TFTP サーバのアドレスを指定します。
interface *interface*	TFTP サーバが存在するインターフェイスを指定します。これは、TFTP サーバの実アドレスにする必要があります。
port	（任意）これは、TFTP サーバが TFTP 要求をリッスンするポートです。デフォルトの TFTP ポート 69 でない場合に、設定する必要があります。

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	トランスペアレント	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

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。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

電話プロキシには、少なくとも 1 つの CUCM TFTP サーバを設定する必要があります。電話プロキシに対して TFTP サーバを 5 つまで設定できます。

TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。TFTP サーバは、CUCM と同じインターフェイス上に存在している必要があります。

内部 IP アドレスを使用して TFTP サーバを作成し、TFTP サーバが存在するインターフェイスを指定します。

IP 電話で、TFTP サーバの IP アドレスを次のように設定する必要があります。

- NAT が TFTP サーバ用に設定されている場合は、TFTP サーバのグローバル IP アドレスを使用します。
- NAT が TFTP サーバ用に設定されていない場合は、TFTP サーバの内部 IP アドレスを使用します。

サービス ポリシーがグローバルに適用されている場合は、TFTP サーバが存在するインターフェイスを除くすべての入力インターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。サービス ポリシーが特定のインターフェイスに適用されている場合は、指定された電話プロキシ モジュールへのインターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。

NAT ルールを TFTP サーバに設定する場合は、分類ルールのインストール時に TFTP サーバのグローバル アドレスが使用されるように、サービス ポリシーを適用する前に、NAT ルールを設定する必要があります。

例

次に、**tftp-server address** コマンドを使用して、電話プロキシに対応する 2 つの TFTP サーバを設定する例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4 interface inside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.25 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# cluster-mode nonsecure
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

threat-detection basic-threat

基本的な脅威の検出をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection basic-threat** コマンドを使用します。基本的な脅威の検出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。

threat-detection basic-threat

no threat-detection basic-threat

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

基本脅威検出は、デフォルトでイネーブルになっています。次のデフォルトのレート制限が使用されます。

表 1-1　基本的な脅威の検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
• アプリケーション インスペクションに不合格のパケット	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。

使用上のガイドライン

基本的な脅威の検出をイネーブルにすると、ASA は、次の理由によるドロップ パケットとセキュリティ イベントのレートをモニタします。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。完全なスキャンによる脅威の検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レート情報を使用し、ホストを攻撃者として分類してそれらのホストを自動的に回避するなどして対処します）。
- 不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

「デフォルト」の項の表 1-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。**threat-detection rate** コマンドを使用して、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、ASA はシステム メッセージを送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。受信するイベントごとに、ASA は平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA はバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにする場合は、グローバル コンフィギュレーション モードで **threat-detection rate** コマンドを使用して、各イベント タイプのデフォルトのレート制限を変更できます。**threat-detection scanning-threat** コマンドを使用してスキャンによる脅威の検出をイネーブルにする場合は、このコマンドに **scanning-threat** キーワードを指定して、ホストを攻撃者またはターゲットと見なすタイミングを設定できます。設定しない場合は、基本的な脅威の検出とスキャンによる脅威の検出の両方で、デフォルトの **scanning-threat** 値が使用されます。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。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

構文の説明

acl-drop	アクセス リストによる拒否のためにドロップされたパケットのレート制限を設定します。
average-rate *av_rate*	平均レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。
bad-packet-drop	パケット形式に誤りがあって（invalid-ip-header や invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレート制限を設定します。
burst-rate *burst_rate*	バースト レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。バースト レートは、*N* 秒ごとの平均レートとして計算されます。*N* はバースト レート間隔です。バースト レート間隔は、**rate-interval** *rate_interval* 値の 1/30 または 10 秒のうち大きい方の値になります。
conn-limit-drop	接続制限（システム全体のリソース制限とコンフィギュレーションで設定される制限の両方）を超えたためにドロップされたパケットのレート制限を設定します。
dos-drop	DoS 攻撃（無効な SPI、ステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレート制限を設定します。
fw-drop	基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレート制限を設定します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	不審な ICMP パケットが検出されたためにドロップされたパケットのレート制限を設定します。
inspect-drop	パケットがアプリケーション インスペクションに失敗したためにドロップされたパケットのレート制限を設定します。
interface-drop	インターフェイスの過負荷が原因でドロップされたパケットのレート制限を設定します。

rate-interval *rate_interval*	平均レート間隔を 600 ～ 2592000 秒（30 日）の範囲で設定します。レート間隔は、ドロップ数の平均値を求める期間を決定するために使用されます。また、バーストしきい値レート間隔を決定します。
scanning-threat	スキャン攻撃が検出されたためにドロップされたパケットのレート制限を設定します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	TCP SYN 攻撃や戻りデータなし UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレート制限を設定します。

デフォルト

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、次のデフォルトのレート制限が使用されます。

表 1-2　基本的な脅威の検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	平均レート	バースト レート
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 100 ドロップ/秒。	直近の 120 秒間で 400 ドロップ/秒。
scanning-threat	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。
syn-attack	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 100 ドロップ/秒。	直近の 120 秒間で 200 ドロップ/秒。
acl-drop	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 400 ドロップ/秒。	直近の 120 秒間で 800 ドロップ/秒。
• **fw-drop** • **inspect-drop**	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 400 ドロップ/秒。	直近の 120 秒間で 1600 ドロップ/秒。
interface-drop	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直近の 3600 秒間で 2000 ドロップ/秒	直近の 120 秒間で 8000 ドロップ/秒。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。

使用上のガイドライン

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

基本的な脅威の検出をイネーブルにした場合、ASA は、「構文の説明」の表で説明したイベント タイプによるドロップ パケットとセキュリティ イベントのレートをモニタします。

ASA は、脅威を検出するとすぐにシステム ログ メッセージ(733100)を送信し、ASDM に警告します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

「デフォルト」の項の表 1-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。

イベント レートが超過すると、ASA はシステム メッセージを送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。受信するイベントごとに、ASA は平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA はバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。

コマンド	説明
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection scanning-threat

スキャンによる脅威の検出をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection scanning-threat** コマンドを使用します。スキャンによる脅威の検出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。

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

構文の説明

duration *seconds*	攻撃元ホストの回避期間を 10 ～ 2592000 秒の範囲で設定します。デフォルトの期間は 3600 秒（1 時間）です。
except	IP アドレスを回避対象から除外します。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。
ip-address *ip_address mask*	回避対象から除外する IP アドレスを指定します。
object-group *network_object_group_id*	回避対象から除外するネットワーク オブジェクト グループを指定します。オブジェクト グループを作成するには、**object-group network** コマンドを参照してください。
shun	ASA がホストを攻撃者であると識別すると、syslog メッセージ 733101 を送信し、さらにホスト接続を自動的に終了します。

デフォルト

デフォルトの回避期間は 3600 秒（1 時間）です。

スキャン攻撃イベントでは、次のデフォルトのレート制限が使用されます。

表 1-3　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**duration** キーワードが追加されました。

使用上のガイドライン

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

注意 スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定したり、自動的にホストを排除したりできます。デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。

ASA は、スキャンによる脅威イベント レートを超過した時点で、攻撃者とターゲットを識別します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。スキャンによる脅威イベントのレート制限は **threat-detection rate scanning-threat** コマンドを使用して変更できます。

攻撃者またはターゲットとして分類されたホストを表示するには、**show threat-detection scanning-threat** コマンドを使用します。

回避対象のホストを表示するには、**show threat-detection shun** コマンドを使用します。排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、スキャンによる脅威の検出をイネーブルにし、10.1.1.0 ネットワーク上のホストを除き、攻撃者として分類されたホストを自動的に回避する例を示します。スキャンによる脅威の検出のデフォルトのレート制限は変更することもできます。

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

関連コマンド

コマンド	説明
clear threat-detection shun	ホストを回避対象から解除します。
show threat-detection scanning-threat	攻撃者およびターゲットとして分類されたホストを表示します。
show threat-detection shun	現在回避されているホストを表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。

threat-detection statistics

高度な脅威の検出の統計情報をイネーブルにするには、グローバル コンフィギュレーション モードで **threat-detection statistics** コマンドを使用します。高度なスキャン脅威検出の統計情報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。

注意 統計情報をイネーブルにすると、イネーブルにした統計情報のタイプに応じて、ASA のパフォーマンスに影響することがあります。**threat-detection statistics host** コマンドはパフォーマンスに大幅に影響を与えるため、トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討します。ただし、**threat-detection statistics port** コマンドは大きな影響を与えません。

threat-detection statistics [**access-list** | [**host** | **port** | **protocol** [**number-of-rate** {**1** | **2** | **3**}] | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

構文の説明

access-list	(任意)アクセス リストによる拒否の統計情報をイネーブルにします。アクセス リスト統計情報は、**show threat-detection top access-list** コマンドを使用した場合にだけ表示されます。
average-rate *attacks_per_sec*	(任意)TCP 代行受信について、syslog メッセージ生成の平均レートしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。
burst-rate *attacks_per_sec*	(任意)TCP 代行受信について、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
host	(任意)ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます(統計情報もクリアされます)。
number-of-rate {**1** | **2** | **3**}	(任意)ホスト、ポート、プロトコルの統計情報に対して維持されるレート間隔の数を設定します。デフォルトのレート間隔の数は **1** です。メモリの使用量を低く抑えます。より多くのレート間隔を表示するには、値を **2** または **3** に設定します。たとえば、値を **3** に設定すると、直前の 1 時間、8 時間、および 24 時間のデータが表示されます。このキーワードを **1** に設定した場合(デフォルト)、最も短いレート間隔統計情報だけが保持されます。値を **2** に設定すると、短い方から 2 つの間隔が保持されます。
port	(任意)ポート統計情報をイネーブルにします。
protocol	(任意)プロトコル統計情報をイネーブルにします。

rate-interval *minutes*	(任意)TCP 代行受信について、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。
tcp-intercept	(任意)TCP 代行受信によって代行受信される攻撃の統計情報をイネーブルにします。TCP 代行受信をイネーブルにするには、**set connection embryonic-conn-max** コマンド、**nat** コマンド、または **static** コマンドを参照してください。

デフォルト

デフォルトでは、アクセス リスト統計情報はイネーブルです。このコマンドにオプションを指定しなかった場合は、すべてのオプションがイネーブルになります。

デフォルトの **tcp-intercept rate-interval** は 30 分です。デフォルトの **burst-rate** は 1 秒あたり 400 です。デフォルトの **average-rate** は 1 秒あたり 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)/8.1(2)	**tcp-intercept** キーワードが追加されました。
8.1(2)	**number-of-rates** キーワードがホスト統計情報用に追加され、レート数のデフォルト値が 3 から 1 に変更されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.3(1)	**number-of-rates** キーワードがポートとプロトコルの統計情報用に追加され、レート数のデフォルト値が 3 から 1 に変更されました。

使用上のガイドライン

このコマンドにオプションを指定しなかった場合は、すべての統計情報がイネーブルになります。特定の統計情報のみをイネーブルにするには、統計情報のタイプごとにこのコマンドを入力します。オプションを指定せずにコマンドを入力しないでください。**threat-detection statistics** を(何もオプションを指定しないで)入力した後、統計情報固有のオプション(たとえば **threat-detection statistics host number-of-rate 2**)を指定してコマンドを入力することで、特定の統計情報をカスタマイズできます。**threat-detection statistics** を(何もオプションを指定しないで)入力した後、特定の統計情報のコマンドを、統計情報固有のオプションを指定しないで入力した場合は、すでにイネーブルになっているので、そのコマンドによる効果は何もありません。

このコマンドの **no** 形式を入力すると、すべての **threat-detection statistics** コマンドが削除されます。これには、デフォルトでイネーブルになる **threat-detection statistics access-list** コマンドも含まれます。

統計情報を表示するには、**show threat-detection statistics** コマンドを使用します。

threat-detection scanning-threat コマンドを使用して、スキャンによる脅威の検出をイネーブルにする必要はありません。検出と統計情報は個別に設定できます。

例

次に、ホストを除くすべてのタイプのスキャンによる脅威の検出とスキャン脅威統計情報の例を示します。

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection statistics access-list
ciscoasa(config)# threat-detection statistics port
ciscoasa(config)# threat-detection statistics protocol
ciscoasa(config)# threat-detection statistics tcp-intercept
```

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection memory	高度な脅威検出の統計情報のメモリ使用を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。

threshold

SLA モニタリング動作のしきい値超過イベントのしきい値を設定するには、SLA モニタ コンフィギュレーション モードで **threshold** 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。

threshold *milliseconds*

no threshold

構文の説明

milliseconds	宣言する上昇しきい値をミリ秒で指定します。有効な値は、0 ～ 2147483647 です。この値は、タイムアウトに設定された値以下にする必要があります。

デフォルト

デフォルトのしきい値は 5000 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

しきい値は、しきい値超過イベントを示すためにだけ使用されます。到達可能性には影響しませんが、**timeout** コマンドの適切な設定を評価するために使用できます。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

throughput level

スマート ライセンス権限付与要求のスループット レベルを設定するには、ライセンス スマート コンフィギュレーション モードで **throughput level** コマンドを使用します。スループット レベルを削除し、デバイスのライセンスを登録解除するには、このコマンドの **no** 形式を使用します。

(注) この機能は、ASAv だけでサポートされています。

throughput level {100M | 1G | 2G}

no throughput level [100M | 1G | 2G]

構文の説明

100M	100 Mbps のスループット レベルを設定します。
1G	1 Gbps のスループット レベルを設定します。
2G	2 Gbps のスループット レベルを設定します。

コマンド 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	トランスペアレント	シングル	コンテキスト	システム
ライセンス スマート コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

スループット レベルを要求または変更する場合、変更を反映させるには、ライセンス スマート コンフィギュレーション モードを終了する必要があります。

例

次に、機能階層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。

ticket（廃止）

Cisco Intercompany Media Engine プロキシ用にチケット エポックとパスワードを設定するには、UC-IME コンフィギュレーション モードで **ticket** コマンドを使用します。プロキシからコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ticket epoch *n* **password** *password*

no ticket epoch *n* **password** *password*

構文の説明

n	パスワードの完全性チェックの時間間隔を設定します。1 ～ 255 の整数を入力します。
password	Cisco Intercompany Media Engine チケットのパスワードを設定します。US-ASCII 文字セットから印刷可能な文字を 10 文字以上 64 文字以下で、入力します。使用可能な文字は 0x21 ～ 0x73 であり、空白文字は除外されます。 パスワードは一度に 1 つしか設定できません。

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	トランスペアレント	シングル	コンテキスト	システム
UC-IME コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine のチケットのエポックとパスワードを設定します。

このエポックには、パスワードが変更されるたびに更新される整数が保管されます。プロキシを初めて設定し、パスワードを初めて入力したとき、エポックの整数として 1 を入力します。このパスワードを変更するたびに、エポックを増やして新しいパスワードを示します。パスワードを変更するたびに、エポックの値を増やす必要があります。

通常、エポックは連続的に増やします。しかし、ASA では、エポックを更新するときに任意の値を選択できます。

エポック値を変更すると、現在のパスワードは無効になり、新しいパスワードを入力する必要があります。

20 文字以上のパスワードを推奨します。パスワードは一度に 1 つしか設定できません。

チケット パスワードはフラッシュ上に保存されます。**show running-config uc-ime** コマンドの出力には、パスワードの文字列ではなく、***** が表示されます。

(注) ASA 上で設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバ上で設定されたエポックおよびパスワードと一致する必要があります。詳細については、Cisco Intercompany Media Engine サーバのマニュアルを参照してください。

例

次の例は、Cisco Intercompany Media Engine プロキシでチケットとエポックを設定する方法を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

timeout（AAA サーバ ホスト）

ASA 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。タイムアウト値を削除し、タイムアウトをデフォルト値の 10 秒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。

timeout *seconds*

no timeout

構文の説明

seconds	サーバのタイムアウト間隔（1 ～ 300 秒）を指定します。各 AAA トランザクションに対して、ASA により、タイムアウトに達するまで（**retry interval** コマンドで定義された間隔に基づいて）接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバ グループ内の **max-failed-attempts** コマンドで指定された制限に達すると、AAA サーバは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバへの要求の送信を開始します。

デフォルト

デフォルトのタイムアウト値は 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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはすべての AAA サーバ プロトコル タイプで有効です。

retry-interval コマンドを使用して、ASA が各接続試行の間で待機する時間を指定できます。これらの間隔は全体的なタイムアウト内で発生するため、再試行間隔を長くすると、システムが全体的なタイムアウト内で行う再試行回数を減らすことができます。実際には、再試行間隔はタイムアウト間隔よりも短くする必要があります。

AAA トランザクションが最大何回連続で失敗したら障害が発生したサーバを非アクティブ化するかを指定するには **max-failed-attempts** コマンドを使用します。AAA トランザクションは、最初の要求と一連の再試行からなるシーケンスです。RADIUS プロトコルの場合、最初の要求とすべての再試行で、RADIUS プロトコル ヘッダーに同じ RADIUS パケット ID が設定されています。

例

次に、ホスト 10.2.3.4 の RADIUS AAA サーバ「svrgrp1」が 30 秒のタイムアウト値と 10 秒の再試行間隔を使用するように設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 10.2.3.4
ciscoasa(config-aaa-server-host)# timeout 30
ciscoasa(config-aaa-server-host)# retry-interval 10
ciscoasa(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	現在の AAA コンフィギュレーションの値を表示します。

timeout（DNS サーバグループ）

次の DNS サーバを試行するまでの待機時間の合計を指定するには、DNS サーバグループ コンフィギュレーション モードで **timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルト値は 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウトは倍増します。dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用して、再試行回数を設定できます。

デフォルト

デフォルトのタイムアウトは 2 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	トランスペアレント	シングル	コンテキスト	システム
DNS サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

次に、DNS サーバ グループ「dnsgroup1」のタイムアウトを 1 秒に設定する例を示します。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# dns timeout 1
```

関連コマンド

コマンド	説明
clear configure dns	ユーザが作成した DNS サーバ グループをすべて削除し、デフォルト サーバ グループの属性をデフォルト値にリセットします。
domain-name	デフォルトのドメイン名を設定します。

コマンド	説明
retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

timeout（グローバル）

さまざまな機能に対応するグローバルな最大アイドル時間を設定するには、グローバル コンフィギュレーション モードで **timeout** コマンドを使用します。すべてのタイムアウト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。単一の機能をデフォルトにリセットするには、**timeout** コマンドにデフォルト値を指定して再度入力します。

timeout {**conn** | **conn-holddown** | **floating-conn** | **h225** | **h323** | **half-closed** | **icmp** | **icmp-error** | **igp stale-route** | **mgcp** | **mgcp-pat** | **pat-xlate** | **sctp** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media** | **sunrpc** | **tcp-proxy-reassembly** | **udp** | **xlate**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

構文の説明

絶対	（**uauth** のオプション）uauth timeout が期限切れになった後、再認証を要求します。デフォルトでは、**absolute** キーワードはイネーブルです。非アクティブな状態が一定時間経過した後 uauth タイマーがタイムアウトするように設定するには、代わりに **inactivity** キーワードを入力します。
conn	接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
conn-holddown	接続に使用されるルートが存在しなくなったり非アクティブな場合に、接続を維持する必要がある時間。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。接続ホールドダウン タイマーの目的は、ルートが発生してすぐにダウンする可能性がある場合に、ルート フラッピングの影響を減らすことです。ルートの収束がもっと早く発生するようにホールドダウン タイマーを減らすことができます。デフォルトは 15 秒です。指定できる範囲は 00:00:00 ～ 00:00:15 です。
floating-conn	同じネットワークへの複数のルートが存在しており、それぞれメトリックが異なる場合、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間で設定します。
hh:*mm*:*ss*	タイムアウトを、時間、分、秒で指定します。接続をタイムアウトしない場合は、**0** を使用します（可能な場合）。
h225	H.225 シグナリング接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。タイムアウト値を 0:0:1 に指定すると、タイマーはディセーブルになり、TCP 接続はすべてのコールがクリアされるとすぐに切断されます。
h323	H.245（TCP）および H.323（UDP）メディア接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。

half-closed	TCP half-closed 接続が解放されるまでのアイドル時間を 0:5:0（9.1(1) 以前の場合）または 0:0:30（9.1(2) 以降の場合）～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
icmp	ICMP のアイドル時間を 0:0:2 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 秒（0:0:2）です。
icmp-error	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間に、0:0:0 ～ 0:1:0 の値、または **timeout icmp** 値のいずれか低い方を指定します。デフォルトは **0**（ディセーブル）です。このタイムアウトが無効で、ICMP インスペクションを有効にすると、ASA では、エコー応答が受信されるとすぐに ICMP 接続を削除します。したがってその（すでに閉じられた）接続用に生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。
igp stale-route	古いルートをルータの情報ベースから削除する前に保持するアイドル時間を指定します。これらのルートは OSPF などの内部ゲートウェイ プロトコル用です。デフォルトは 70 秒（00:01:10）です。指定できる範囲は 00:00:10 ～ 00:01:40 です。
inactivity	（**uauth** のオプション）非アクティブ タイムアウトが期限切れになった後、uauth 再認証を要求します。
mgcp	MGCP メディア接続を削除するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは、5 分（0:5:0）です。
mgcp-pat	MGCP PAT 変換を削除するまでの絶対間隔を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 5 分（0:5:0）です。
pat-xlate	PAT 変換スロットが解放されるまでのアイドル時間を 0:0:30 ～ 0:5:0 の範囲で指定します。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。
sctp	Stream Control Transmission Protocol（SCTP）の接続が閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の間で指定します。デフォルトは 2 分（0:2:0）です。
sip	SIP 制御接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、30 分（0:30:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
sip-disconnect	CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間を 0:0:1 ～ 00:10:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sip-invite	（任意）暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、3 分（0:3:0）です。
sip_media	SIP メディア接続を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。 SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
sip-provisional-media	SIP プロビジョナル メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。

sunrpc	SUNRPC スロットを閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
tcp-proxy-reassembly	再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
uauth	認証および認可キャッシュがタイムアウトし、ユーザが次回接続時に再認証が必要となるまでの継続時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。デフォルトのタイマーは **absolute** です。**inactivity** キーワードを入力すると、非アクティブになってから一定の期間後にタイムアウトが発生するように設定できます。**uauth** 継続時間は、**xlate** 継続時間より短く設定する必要があります。キャッシュをディセーブルにするには、**0** に設定します。接続に受動 FTP を使用している場合、または Web 認証に **virtual http** コマンドを使用している場合は、**0** を使用しないでください。
udp	UDP スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
xlate	変換スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 3 時間（3:0:0）です。

デフォルト

デフォルトの設定は次のとおりです。

- **conn** は 1 時間（**1:0:0**）です。
- **conn-holddown** は 15 秒（**0:0:15**）です。
- **floating-conn** はタイムアウトになりません（**0**）。
- **h225** は 1 時間（**1:0:0**）です。
- **h323** は 5 分（**0:5:0**）です。
- **half-closed** は 10 分（**0:10:0**）です。
- **icmp** は 2 秒（**0:0:2**）です。
- **icmp-error** はタイムアウトになりません（**0**）。
- **igp stale-route** は 70 秒（**00:01:10**）です。
- **mgcp** は 5 分（**0:5:0**）です。
- **mgcp-pat** は 5 分（**0:5:0**）です。
- **rpc** は 5 分（**0:5:0**）です。
- **sctp** は 2 分（**0:2:0**）です。
- **sip** は 30 分（**0:30:0**）です。
- **sip-disconnect** は 2 分（**0:2:0**）です。
- **sip-invite** は 3 分（**0:3:0**）です。
- **sip_media** は 2 分（**0:2:0**）です。
- **sip-provisional-media** は 2 分（**0:2:0**）です。
- **sunrpc** は 10 分（**0:10:0**）です。
- **tcp-proxy-reassembly** は 1 分（**0:1:0**）です。

- **uauth** は 5 分（**0:5:0**）**絶対時間**です。
- **udp** は 2 分（**0:02:0**）です。
- **xlate** は 3 時間（**3:0:0**）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	トランスペアレント	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 モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	**mgcp-pat**、**sip-disconnect**、および **sip-invite** キーワードが追加されました。
7.2(4)/8.0(4)	**sip-provisional-media** キーワードが追加されました。
7.2(5)/8.0(5)/8.1(2)/8.2(1)	**tcp-proxy-reassembly** キーワードが追加されました。
8.2(5)/8.4(2)	**floating-conn** キーワードが追加されました。
8.4(3)	**pat-xlate** キーワードが追加されました。
9.1(2)	最小 **half-closed** 値が 30 秒（0:0:30）に引き下げられました。
9.4(3)/9.6(2)	**conn-holddown** キーワードが追加されました。
9.5(2)	**sctp** キーワードが追加されました。
9.7(1)	**igp stale-route** キーワードが追加されました。
9.8(1)	**icmp-error** キーワードが追加されました。

使用上のガイドライン

timeout コマンドを使用すると、グローバルにタイムアウトを設定できます。一部の機能では、コマンドで指定されたトラフィックに対し、**set connection timeout** コマンドが優先されます。

timeout コマンドの後に、キーワードと値を複数入力できます。

接続タイマー（**conn**）は変換タイマー（**xlate**）より優先されます。変換タイマーは、すべての接続がタイムアウトになった後にのみ動作します。

例

次に、最大アイドル時間を設定する例を示します。

```
ciscoasa(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
ciscoasa(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

関連コマンド

コマンド	説明
clear configure timeout	タイムアウト コンフィギュレーションをクリアし、デフォルトにリセットします。
set connection timeout	Modular Policy Framework を使用して接続タイムアウトを設定します。
show running-config timeout	指定されたプロトコルのタイムアウト値を表示します。

timeout（policy-map type inspect gtp > パラメータ）

GTP セッションの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** 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 モードにアクセスするには、まず **policy-map type inspect gtp** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

no timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	指定したサービスのアイドル タイムアウト（時間:分:秒の形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。
endpoint	GTP エンドポイントが削除されるまでの非アクティブ時間の最大値。
gsn	GSN が削除されるまでの非アクティブ時間の最大値。 9.5(1) 以降、このキーワードは削除され、**endpoint** キーワードに置き換えられました。
pdp-context	GTP セッションの PDP コンテキストを削除するまでの非アクティブ時間の最大値。GTPv2 では、これはベアラー コンテキストです。
request	要求キューから要求が削除されるまでの非アクティブ時間の最大値。廃棄された要求に対する後続の応答もすべて廃棄されます。
signaling	GTP シグナリングが削除されるまでの非アクティブ時間の最大値。
t3-response	接続を除去する前に応答を待機する最大時間。
tunnel	GTP トンネルが切断されるまでの非アクティブ時間の最大値。

デフォルト

endpoint、**gsn**、**pdp-context**、および **signaling** のデフォルトは 30 分です。

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 時間です（PDP コンテキスト削除要求を受信しない場合）。

t3-response のデフォルトは、20 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	**gsn** キーワードは **endpoint** に置き換えられました。

使用上のガイドライン

GTP インスペクションで使用されるデフォルト タイムアウトを変更するには、このコマンドを使用します。

例

次に、要求キューのタイムアウト値を 2 分に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout request 00:02:00
```

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。
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。

timeout（policy-map type inspect m3ua > パラメータ）

M3UA セッションの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** 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 モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**endpoint** | **session**} *hh*:*mm*:*ss*

no timeout {**endpoint** | **session**} *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	指定したサービスのアイドル タイムアウト（時間:分:秒の形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。
endpoint	M3UA エンドポイントの統計情報が削除されるまでの非アクティブ時間の最大値。デフォルトは 30 分です。
session	厳密な ASP 状態の確認を有効にしている場合の、M3UA セッションを削除するためのアイドル タイムアウト（hh:mm:ss の形式）。デフォルトは 30 分（0:30:00）です。このタイムアウトを無効にすると、失効したセッションの削除を防止できます。

デフォルト

endpoint および **session** のデフォルトは 30 分です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。
9.7(1)	**session** キーワードが追加されました。

使用上のガイドライン

M3UA インスペクションで使用されるデフォルト タイムアウトを変更するには、このコマンドを使用します。

例

次の例では、45 分のエンドポイントのタイムアウトを設定します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
show service-policy inspect m3ua	M3UA 統計情報を表示します。
strict-asp-state	厳密な M3UA ASP 状態検証をイネーブルにします。

timeout（policy-map type inspect radius-accounting > パラメータ）

RADIUS アカウンティング ユーザの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** 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 モードにアクセスするには、まず **policy-map type inspect radius-accounting** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン(:)で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。デフォルトは 1 時間です。
users	ユーザのタイムアウトを指定します。

デフォルト

ユーザのデフォルトのタイムアウトは 1 時間です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ユーザのタイムアウト値を 10 分に設定する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout user 00:10:00
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

timeout（type echo）

SLA 動作が要求パケットへの応答を待機する時間を設定するには、type echo コンフィギュレーション モードで **timeout** コマンドを使用します。type echo コンフィギュレーション モードにアクセスするには、まず **sla monitor** コマンドを入力します。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。

timeout *milliseconds*

no timeout

構文の説明

milliseconds	0 ～ 604800000

デフォルト

デフォルトのタイムアウト値は 5000 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
Type echo コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

frequency コマンドを使用して、SLA 動作が要求パケットを送信する頻度を設定し、**timeout** コマンドを使用して、SLA 動作がそれらの要求への応答の受信を待機する時間を設定できます。**timeout** コマンドには、**frequency** コマンドに指定する値より大きい値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
sla monitor	SLA モニタリング動作を定義します。

timeout assertion

SAML タイムアウトを設定するには、webvpn コンフィギュレーション モードで **timeout assertion** コマンドを使用します。

timeout assertion *number of seconds*

構文の説明

number of seconds	SAML IdP タイムアウト(秒)。

デフォルト

デフォルトは、なしです。アサーションの NotBefore と NotOnOrAfter によって有効期間が決定されることを意味します。

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	トランスペアレント	シングル	コンテキスト	システム
config webVPN	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5.2	このコマンドが追加されました。

使用上のガイドライン

指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。config-webvpn-saml-idp でタイムアウト値を入力する場合、アサーションと秒数の両方が必要です。

例

次に、クライアントレス VPN ベースの URL、SAML 要求署名、および SAML アサーション タイムアウトの設定例を示します。

```
ciscoasa(config-webvpn-saml-idp)# base url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

timeout edns

サーバからの応答がない場合に、クライアントから Umbrella サーバへの接続を削除するまでのアイドル タイムアウトを設定するには、Umbrella コンフィギュレーション モードで **timeout edns** 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。

timeout edns *hh*:*mm*:*ss*

no timeout edns *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	クライアントから Umbrella サーバへの接続のアイドル タイムアウト（時間:分:秒の形式）、0:0:0 ～ 1193:0:0。デフォルトは 0:02:00（2 分）です。タイムアウトを設定しない場合は、番号に 0 を指定します。

デフォルト

デフォルトは 0:02:00（2 分）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	トランスペアレント	シングル	コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

例

次の例では、クライアントから Umbrella サーバへの接続に、1 分間のアイドル タイムアウトを設定します。

```
ciscoasa(config)# umbrella-global
ciscoasa(config)# timeout edns 0:1:0
```

関連コマンド

コマンド	説明
public-key	Cisco Umbrella で使用する公開キーを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

timeout pinhole

DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きするには、パラメータ コンフィギュレーション モードで **timeout pinhole** 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。

timeout pinhole *hh:mm:ss*

no timeout pinhole

構文の説明

hh:mm:ss	ピンホール接続のタイムアウト。指定できる値は 0:0:1 ～ 1193:0:0 です。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、DCERPC インスペクション ポリシー マップでピンホール接続のピンホール タイムアウトを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
```

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。

timeout secure-phones（廃止）

電話プロキシ データベースからセキュア フォン エントリを削除するまでのアイドル タイムアウトを設定するには、電話プロキシ コンフィギュレーション モードで **timeout secure-phones** コマンドを使用します。タイムアウト値をデフォルトの 5 分に戻すには、このコマンドの **no** 形式を使用します。

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

構文の説明

hh:mm:ss	オブジェクトを削除するまでのアイドル タイムアウトを指定します。デフォルトは 5 分です。

デフォルト

セキュア フォン タイムアウトのデフォルト値は 5 分です。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

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。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。エントリのタイムスタンプは、電話プロキシが SIP 電話の登録更新および SCCP 電話のキープアライブを受信するたびに更新されます。

timeout secure-phones コマンドのデフォルト値は 5 分です。SCCP キープアライブおよび SIP レジスタ更新の最大タイムアウト値より大きい値を指定します。たとえば、SCCP キープアライブが 1 分間隔に指定され、SIP レジスタ更新が 3 分に設定されている場合は、このタイムアウト値には 3 分より大きい値を設定します。

例

次に、**timeout secure-phones** コマンドを使用して、電話プロキシが 3 分後にセキュア フォン データベースのエントリをタイムアウトにするように設定する例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# timeout secure-phones 00:03:00
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

time-range

時間範囲コンフィギュレーション モードを開始し、トラフィック ルールにアタッチできる時間範囲、またはアクションを定義するには、グローバル コンフィギュレーション モードで **time-range** コマンドを使用します。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。

time-range *name*

no time-range *name*

構文の説明

name　時間範囲の名前。名前は 64 文字以下にする必要があります。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

時間範囲を作成してもデバイスへのアクセスは制限されません。**time-range** コマンドは時間範囲のみを定義します。時間範囲を定義した後、それをトラフィック ルールまたはアクションにアタッチできます。

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

時間範囲はASAのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次に、時間範囲「New_York_Minute」を作成し、時間範囲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。

```
ciscoasa(config)# time-range New_York_Minute
ciscoasa(config-time-range)#
```

時間範囲を作成し、時間範囲コンフィギュレーション モードを開始した後、**absolute** コマンドと **periodic** コマンドを使用して時間範囲パラメータを定義できます。**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。その後、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

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

ACL の詳細については、**access-list extended** コマンドを参照してください。

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
access-list extended	ASA 経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。

timers nsf wait

nsf 待機タイマーを調整するには、ルータ OSPF コンフィギュレーション モードで **timers nsf wait** コマンドを使用します。OSPF のタイミングをデフォルト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。

timers nsf wait *interval*

no timers nsf-wait *interval*

構文の説明

間隔	NSF 再起動中のインターフェイス待機間隔（秒単位）。デフォルトは 20 秒です。範囲は 0 ～ 65535 です。

デフォルト

nsf 待機タイマーのデフォルト値は 20 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	トランスペアレント	シングル	コンテキスト	システム
ルータ OSPF コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF ルータでは、すべてのネイバーがパケットに含まれているかが不明な場合は、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが予期されます。ただし、隣接関係（アジャセンシー）を維持するにはルータの再起動が必要です。RS ビット値は RouterDeadInterval 秒より長くすることはできません。Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するには、**timer nsf wait** コマンドを使用します。

例

次に、nsf 待機間隔を秒単位で設定する例を示します。

```
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# timers ?

router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
```

```
ciscoasa(config-router)# timers nsf ?

router mode commands/options:
  wait  Interface wait interval during NSF restart
ciscoasa(config-router)# timers nsf wait ?

router mode commands/options:
  <1-65535>  Seconds
ciscoasa(config-router)# timers nsf wait 35
ciscoasa(config-router)#
```

timers bgp

BGP ネットワーク タイマーを調整するには、ルータ BGP コンフィギュレーション モードで **timers bgp** コマンドを使用します。BGP のタイミングをデフォルト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。

timers bgp *keepalive holdtime* [*min-holdtime*]

no timers bgp *keepalive holdtime* [*min-holdtime*]

構文の説明

Keepalive（キープアライブ）	Cisco IOS ソフトウェアがピアにキープアライブ メッセージを送信する頻度（秒単位）。デフォルトは 60 秒です。範囲は 0 ～ 65535 です。
holdtime	キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであるとソフトウェアが宣言するまでの時間（秒単位）。デフォルトは 180 秒です。範囲は 0 ～ 65535 です。
min-holdtime	（オプション）BGP ネイバーからの最小許容ホールド タイムを指定する間隔（秒単位）。最小許容ホールド タイムは、*holdtime* 引数で指定された間隔以下にする必要があります。範囲は 0 ～ 65535 です。

デフォルト

keepalive：60 秒
holdtime：180 秒

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	トランスペアレント	シングル	コンテキスト	システム
ルータ BGP コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

holdtime 引数を 20 秒未満の値の値に設定すると、次の警告が表示されます。「A hold time of less than 20 seconds increases the chances of peer flapping」

最小許容ホールド タイム間隔が、指定されたホールド タイムを超過する場合は、「Minimum acceptable hold time should be less than or equal to the configured hold time」という通知が表示されます。

（注） BGP ルータに最小許容ホールド タイムが設定されている場合、リモート BGP ピア セッションは、リモート ピアが最小許容ホールド タイム間隔以上のホールド タイムをアドバタイズする場合にのみ確立されます。最小許容ホールド タイム間隔が、設定されたホールド タイムを超過する場合、次回のリモート セッション確立の試行は失敗し、ローカル ルータは「unacceptable hold time」という示す通知を送信します。

例

次に、キープアライブ タイマーを 70 秒、ホールド タイム タイマーを 130 秒、最小許容ホールド タイム間隔を 100 秒に変更する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# timers bgp 70 130 100
```

timers lsa arrival

ASA が OSPFv3 ネイバーから同じ LSA を受信する最小間隔を設定するには、IPv6 ルータ コンフィギュレーション モードで **timers lsa arrival** 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。

timers lsa arrival *milliseconds*

no timers lsa arrival *milliseconds*

構文の説明

milliseconds	ネイバー間で着信する同じ LSA を受信する間に経過する必要がある最小遅延を指定します（ミリ秒単位）。有効値の範囲は 0 ～ 600,000 ミリ秒です。

デフォルト

デフォルトは 1000 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマン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して、ネイバーから着信する同じ LSA を受信する間に経過する必要がある最小間隔を指定します。

例

次に、同じ LSA を受信する最小間隔を 2000 ミリ秒に設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# timers lsa arrival 2000
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 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 ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。

timers lsa-group-pacing

OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、ルータ コンフィギュレーション モードで **timers lsa-group-pacing** 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。

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

構文の説明

seconds	OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を変更するには **timers lsa-group-pacing** *seconds* コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers lsa-group-pacing** コマンドを使用します。

例

次に、LSA のグループ処理間隔を 500 秒に設定する例を示します。

```
ciscoasa(config-rtr)# timers lsa-group-pacing 500
ciscoasa(config-rtr)#
```

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。
timers spf	最短パス優先（SPF）計算遅延とホールド タイムを指定します。

timers pacing flood

LSA フラッド パケット ペーシングを設定するには、IPv6 ルータ コンフィギュレーション モードで **timers pacing flood** コマンドを使用します。デフォルトのフラッド パケット ペーシング値に戻すには、このコマンドの **no** 形式を使用します。

timers pacing flood *milliseconds*

no timers pacing flood *milliseconds*

構文の説明

milliseconds	フラッディング キュー内の LSA がアップデート間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。

デフォルト

デフォルトは 33 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマン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して、LSA フラッド パケット ペーシングを設定します。

例

次の例は、OSPFv3 に対して LSA フラッド パケット ペーシング更新が 20 ミリ秒間隔で発生する設定を示しています。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
timers pacing lsa-group	OSPFv3 LSA を収集してグループ化し、更新、チェックサム、または期限切れにする間隔を指定します。

timers pacing flood

LSA フラッド パケット ペーシングを設定するには、IPv6 ルータ コンフィギュレーション モードで **timers pacing flood** コマンドを使用します。デフォルトのフラッド パケット ペーシング値に戻すには、このコマンドの **no** 形式を使用します。

timers pacing flood *milliseconds*

no timers pacing flood *milliseconds*

構文の説明

milliseconds	フラッディング キュー内の LSA がアップデート間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。

デフォルト

デフォルトは 33 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマン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して、LSA フラッド パケット ペーシングを設定します。

例

次の例は、OSPFv3 に対して LSA フラッド パケット ペーシング更新が 20 ミリ秒間隔で発生する設定を示しています。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
timers pacing lsa-group	OSPFv3 LSA を収集してグループ化し、更新、チェックサム、または期限切れにする間隔を指定します。

timers pacing lsa-group

OSPFv3 LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、IPv6 ルータ コンフィギュレーション モードで **timers pacing lsa-group** 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。

timers pacing lsa-group *seconds*

no timers pacing lsa-group [*seconds*]

構文の説明

seconds	LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定します（秒単位）。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマン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して、OSPFv3 LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定します。

例

次に、OSPFv3 ルーティング プロセス 1 に対して、LSA グループ間の OSPFv3 グループ パケット ペーシング更新が 300 秒間隔で発生するように設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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 ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。
timers pacing retransmission	LSA 再送信パケット ペーシングを設定します。

timers pacing retransmission

リンクステート アドバタイズメント（LSA）の再送信パケット ペーシングを設定するには、ルータ コンフィギュレーション モードで **timers pacing retransmission** コマンドを使用します。デフォルトの再送信パケット ペーシング値に戻すには、このコマンドの **no** 形式を使用します。

timers pacing retransmission *milliseconds*

no timers pacing retransmission

構文の説明

milliseconds	再送信キュー内の LSA がペーシング処理される間隔を指定します（ミリ秒単位）。有効な値は、5 ～ 200 ミリ秒です。

デフォルト

デフォルトの間隔は 66 ミリ秒です。

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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

Open Shortest Path First（OSPF）再送信ペーシング タイマーを設定すると、OSPF 伝送キュー内の連続リンクステート アップデート パケット間のパケット間スペースを制御できます。このコマンドを使用すると、LSA 更新が発生するレートを制御できます。したがって、エリアが非常に多くの数の LSA で満たされた場合に発生する可能性のある、CPU またはバッファの高い使用率を低減させることができます。OSPF パケット再送信ペーシング タイマーのデフォルト設定は、大半の OSPF 配備に適しています。

（注） OSPF パケット フラッディングの要件を満たす他のオプションをすべて使用した場合に限り、パケット再送信ペーシング タイマーを変更してください。特に、ネットワーク オペレータは、デフォルトのフラッディング タイマーを変更する前に、集約、スタブ エリアの使用方法、キューの調整、およびバッファの調整を優先して行う必要があります。

さらに、タイマー値を変更するガイドラインはなく、各 OSPF 配備は一意であり、ケースバイケースで考慮する必要があります。ネットワーク オペレータは、デフォルトのパケット再送信ペーシング タイマー値を変更することで生じるリスクを念頭に置く必要があります。

例

次に、OSPF ルーティング プロセス 1 に対して、LSA フラッド ペーシング更新が 55 ミリ秒間隔で発生するように設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# timers pacing retransmission 55
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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 ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。

timers spf

最短パス優先(SPF)計算遅延とホールド タイムを指定するには、ルータ コンフィギュレーション モードで **timers spf** 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。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

構文の説明

delay	OSPF がトポロジ変更を受信してから最短パス優先(SPF)計算を開始するまでの遅延時間を 1 ～ 65535 の範囲(秒単位)で指定します。
holdtime	2 つの連続する SPF 計算の間のホールド タイム(秒単位)。有効な値は、1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

- *delay* は 5 秒です。
- *holdtime* 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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

OSPF プロトコルがトポロジ変更を受信してから計算を開始するまでの遅延時間と、2 つの連続する SPF 計算の間のホールド タイムを設定するには、**timers spf** コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers spf** コマンドを使用します。

例

次に、SPF 計算遅延を 10 秒に設定し、SPF 計算ホールド タイムを 20 秒に設定する例を示します。

```
ciscoasa(config-router)# timers spf 10 20
ciscoasa(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。
timers lsa-group-pacing	OSPF リンク ステート アドバタイズメント（LSA）を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

timers throttle

Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）の生成または SPF の生成に関するレート制限値を設定するには、ルータ OSPF または IPv6 ルータ OSPF コンフィギュレーション モードで **timers throttle** 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。

timers throttle {**lsa** | **spf**} *start-interval hold-interval max-interval*

no timers throttle {**lsa** | **spf**}

構文の説明

lsa	LSA スロットリングを設定します。
start-interval	LSA の最初のオカレンスを生成する遅延を指定します（ミリ秒単位）。SPF 計算への変更を受信する遅延を指定します（ミリ秒単位）。 LSA の最初のオカレンスを生成する最小遅延を指定します（ミリ秒単位）。 （注） LSA の最初のインスタンスは、ローカル OSPF トポロジの変更直後に生成されます。次の LSA は、*start-interval* の後にのみ生成されます。 有効な値は、0 ～ 600,000 ミリ秒です。デフォルト値は 0 ミリ秒です。LSA は即座に送信されます。
hold-interval	同じ LSA を発信する最大遅延を指定します（ミリ秒単位）。1 番目と 2 番目の SPF 計算間の遅延を指定します（ミリ秒単位）。 LSA を生成する最小遅延を再度指定します（ミリ秒単位）。この値は、LSA 生成の後続のレート制限時間の計算に使用されます。有効な値は、1 ～ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
max-interval	同じ LSA を発信する最小遅延を指定します（ミリ秒単位）。SPF 計算を待機する最大時間を指定します（ミリ秒単位）。 LSA を生成する最大遅延を再度指定します（ミリ秒単位）。有効な値は、1 ～ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
spf	SPF スロットリングを設定します。

デフォルト

LSA スロットリング:

- *start-interval* の場合、デフォルト値は 0 ミリ秒です。
- *hold-interval* の場合、デフォルト値は 5000 ミリ秒です。
- *max-interval* の場合、デフォルト値は 5000 ミリ秒です。

SPF スロットリング:

- *start-interval* の場合、デフォルト値は 5000 ミリ秒です。
- *hold-interval* の場合、デフォルト値は 10000 ミリ秒です。
- *max-interval* の場合、デフォルト値は 10000 ミリ秒です。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.2(1)	IPv6 のサポートが追加されました。

使用上のガイドライン

LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPF の LSA 更新速度を低下し、ミリ秒単位の LSA レート制限を提供することにより、より高速な OSPF コンバージェンスを許可するダイナミック メカニズムを提供します。

LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPF が自動的に最初のオカレンス値に修正します。同様に、指定された最大遅延が最小遅延よりも小さい場合、OSPF が自動的に最小遅延値に修正します。

SPF スロットリングでは、*hold-interval* または *max-interval* が *start-interval* よりも小さい場合、OSPF が自動的に *start-interval* の値に修正します。同様に、*max-interval* が *hold-interval* よりも小さい場合、OSPF が自動的に *hold-interval* の値に修正します。

例

次に、OSPFv3 LSA スロットリングをミリ秒単位で設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 4000 5000
```

次に、LSA スロットリングで、指定された最大遅延値が最小遅延値を下回る場合に発生する自動修正の例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle lsa 100 100 100
```

次に、OSPFv3 SPF スロットリングをミリ秒単位で設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

次に、SPF スロットリングで、指定された最大遅延値が最小遅延値を下回る場合に発生する自動修正の例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle spf 100 100 100
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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 ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
timers lsa-group-pacing	OSPFv3 LSA を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

timestamp

IP オプション インスペクションにおいて、パケット ヘッダー内にタイム スタンプ（TS）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **timestamp** 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。

timestamp action {allow | clear}

no timestamp action {allow | clear}

構文の説明

allow	タイム スタンプ IP オプションを含むパケットを許可します。
clear	パケット ヘッダーからタイム スタンプ オプションを削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、タイム スタンプ オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timestamp action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

title

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示する WebVPN ページのタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **title** コマンドを使用します。

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトル テキストは「WebVPN Service」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

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	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

タイトルを付けない場合は、*value* 引数を指定せずに **title text** コマンドを使用します。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次の例では、タイトルがテキスト「Cisco WebVPN Service」でカスタマイズされています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# title text Cisco WebVPN Service
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
page style	カスケーディング スタイル シート（CSS）パラメータを使用して WebVPN ページをカスタマイズします。

tls-proxy コマンド～ type echo コマンド

tls-proxy

TLS コンフィギュレーション モードで TLS プロキシ インスタンスを設定したり、最大セッション数を設定したりするには、グローバル コンフィギュレーション モードで **tls-proxy** コマンドを使用します。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。

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

構文の説明

max_sessions *max_sessions*	プラットフォームでサポートする TLS プロキシ セッションの最大数を指定します。
noconfirm	確認を要求せずに **tls-proxy** コマンドを実行します。
proxy_name	TLS プロキシ インスタンス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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

tls-proxy コマンドを使用して TLS プロキシ コンフィギュレーション モードを開始し、TLS プロキシ インスタンスを作成したり、プラットフォームでサポートされる最大セッション数を設定したりできます。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
クライアント	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキー ペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。

token

Cisco Umbrella に登録するために必要な API トークンを設定するには、Umbrella コンフィギュレーション モード で **token** コマンドを使用します。トークンを削除するには、このコマンドの **no** 形式を使用します。

token *api_token*

no token *api_token*

構文の説明

api-token	Cisco Umbrella への登録に必要な API トークン。Cisco Umbrella ネットワーク デバイス ダッシュ ボード（https://login.umbrella.com/）からトークンを取得する必要があります。トークンは、16 進数の文字列、たとえば、AABBA59A0BDE1485C912AFE になります。

デフォルト

デフォルトの API トークンはありません。

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	トランスペアレント	シングル	コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Umbrella にデバイスを正常に登録するには、API トークンを設定する必要があります。トークンは顧客ごとに一意であり、デバイスごとに一意ではありません。

登録は、スタンドアロン デバイス、クラスタ、またはフェールオーバー グループに対して行われます。クラスタまたはフェールオーバー グループ内の各デバイスを個別に登録はしません。マルチ コンテキスト モードでは、各コンテキストは、スタンドアロンか、クラスタまたはフェールオーバー グループ内に存在するかに関わらず、デバイスです。

例

次の例では、API トークンを Cisco Umbrella に登録するよう設定します。

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

関連コマンド

コマンド	説明
public-key	Cisco Umbrella で使用する公開キーを設定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

tos

SLA 動作要求パケットの IP ヘッダー内のタイプ オブ サービス バイトを定義するには、SLA モニタ プロトコル コンフィギュレーション モードで **tos** 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。

tos *number*

no tos

構文の説明

number	IP ヘッダーで使用するサービス タイプの値。有効な値は、0 ～ 255 です。

デフォルト

デフォルトのタイプ オブ サービス値は 0 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。これは、専用アクセス レートなどのポリシー ルーティングおよび機能のために、ネットワーク上の他のルータによって使用されます。

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。エコー要求パケットのペイロード サイズを 48 バイトに設定し、SLA 動作中に送信されるエコー要求数を 5 に、さらにタイプ オブ サービス バイトを 80 に設定します。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# tos 80
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
```

```
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(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。
request-data-size	要求パケットのペイロードのサイズを指定します。
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。

traceroute

パケットが宛先に到達するまでのルートを特定するには、**traceroute** コマンドを使用します。

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

構文の説明

destination_ip	traceroute の宛先 IP アドレスを指定します。IPv4 アドレスと IPv6 アドレスの両方をサポートします。
hostname	ルートをトレースする先のホストのホスト名。ホストの宛先には、IPv4 または IPv6 アドレスを使用できます。ホスト名を指定する場合は、**name** コマンドで定義するか、traceroute をイネーブルにしてホスト名を IP アドレスに解決するように DNS サーバを設定します。www.example.com などの DNS ドメイン名をサポートします。
max-ttl	使用可能な最大 TTL 値。デフォルトは 30 です。traceroute パケットが宛先に到達するか、値に達したときにコマンドは終了します。
min_ttl	最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホップの表示を抑制するためにより大きい値を設定できます。
numeric	出力に中間ゲートウェイの IP アドレスのみが示されるように指定します。このキーワードを指定しない場合は、トレース中に到達したゲートウェイのホスト名の検索を試みます。
port *port_value*	ユーザ データグラム プロトコル(UDP)プローブ メッセージによって使用される宛先ポート。デフォルトは 33434 です。
probe *probe_num*	TTL の各レベルで送信するプローブの数。デフォルト数は 3 です。
source	トレース パケットの送信元として使用される IP アドレスまたはインターフェイスを指定します。IPv6 では、IPv6 送信元アドレスのみが受け入れられます。
source_interface	パケット トレースの送信元インターフェイスを指定します。指定する場合は、送信元インターフェイスの IP アドレスが使用されます。
source_ip	パケット トレースの送信元 IP アドレスを指定します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードの場合は、ASA の管理 IP アドレスにする必要があります。
timeout	使用されるタイムアウト値を指定します。
timeout_value	接続をタイムアウトにする前に応答を待機する時間を指定します。デフォルトは 3 秒です。
ttl	プローブで使用する存続可能時間の値の範囲を指定するキーワード。
use-icmp	UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するように指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.7.(1)	このコマンドは、IPv6 アドレスを受け入れるように更新されました。

使用上のガイドライン

traceroute コマンドは送信した各プローブの結果を示します。出力の各行が 1 つの TTL 値に対応します(昇順)。次に、**traceroute** コマンドによって表示される出力記号を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
U	宛先へのルートが存在しません。
nn msec	各ノードに対する、指定した数のプローブのラウンドトリップ時間(ミリ秒)。
!N.	ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。ICMPv6 では、ポートが到達不能です。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

例

次に、宛先 IP アドレスを指定した場合の traceroute 出力の例を示します。

```
ciscoasa# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

```
ciscoasa/admin(config)# traceroute 2002::130
Type escape sequence to abort.
Tracing the route to 2002::130
 1  5000::2 0 msec 0 msec 0 msec
2  2002::130 10 msec 0 msec 0 msec
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
packet-tracer	パケット トレース機能をイネーブルにします。

track rtr

SLA 動作の到達可能性を追跡するには、グローバル コンフィギュレーション モードで **track rtr** コマンドを使用します。SLA 追跡を削除するには、このコマンドの **no** 形式を使用します。

track *track-id* **rtr** *sla-id* **reachability**

no track *track-id* **rtr** *sla-id* **reachability**

構文の説明

reachability	オブジェクトの到達可能性を追跡するように指定します。
sla-id	トラッキング エントリが使用する SLA の ID。
track-id	トラッキング エントリ オブジェクト ID を作成します。有効な値は、1 ～ 500 です。

デフォルト

SLA 追跡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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

track rtr コマンドは、トラッキング エントリ オブジェクト ID を作成し、トラッキング エントリが使用する SLA を指定します。

各 SLA 動作が、トラッキング プロセスによって解釈される動作戻りコード値を維持します。戻りコードには、OK や Over Threshold などのいくつかの戻りコードがあります。表 2-1 は、これらの戻りコードに関連するオブジェクトの到達可能性ステートを表示します。

表 2-1　SLA 追跡の戻りコード

トラッキング	戻りコード	追跡ステート
到達可能性	OK または Over Threshold	Up
	他の任意のコード	Down

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
route	スタティック ルートを設定します。
sla monitor	SLA モニタリング動作を定義します。

traffic-forward

トラフィックをモジュールに転送し、アクセス制御とその他の処理をバイパスするには、インターフェイス コンフィギュレーション モードで **traffic-forward** コマンドを使用します。トラフィック転送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。

traffic-forward *module_type* **monitor-only**

no traffic-forward *module_type* **monitor-only**

構文の説明

module_type	モジュールのタイプサポートされるモジュールは次のとおりです。 • **sfr**：ASA FirePOWER モジュール。 • **cxsc**：ASA CX モジュール。
monitor-only	モジュールをモニタ専用モードに設定します。モニタ専用モードでは、モジュールはトラフィックを処理できますが、その後トラフィックをドロップします。モジュール タイプによって使用方法は異なります。 • ASA FirePOWER：このコマンドを使用して、パッシブ モードを設定します。このモードは実稼働用に使用できます。 • ASA CX：これは厳密にはデモンストレーション モードです。トラフィック転送インターフェイスまたはデバイスを実稼働用に使用することはできません。

コマンド 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	トランスペアレント	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	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。
9.2(1)	**sfr** キーワードが追加されました。
9.3(2)	**sfr** キーワードの実稼働用の使用のサポートが追加されました。

使用上のガイドライン

monitor-only キーワードを指定してサービス ポリシーの **sfr** または **cxsc** コマンドを使用する代わりに、このコマンドでトラフィックをモジュールにリダイレクトできます。サービス ポリシーにより、トラフィックは依然として、廃棄トラフィックを生じる可能性があるアクセス ルールや TCP 正規化などの ASA の処理が前提となっています。さらに、ASA はトラフィックのコピーを単純にモジュールに送信して、最終的にはそれ自身のポリシーに従ってトラフィックを送信します。

一方で、**traffic-forward** コマンドは ASA 処理を完全にバイパスして、トラフィックを単純にモジュールに転送します。モジュールは、トラフィックを検査し、ポリシーを決定し、イベントを生成して、インライン モードで動作した場合に、トラフィックに対してどのような処理が行われることになるかを示します。モジュールはトラフィックのコピーに対して動作しますが、ASA 自体は、ASA またはモジュールのポリシー決定に関係なくトラフィックを即座にドロップします。モジュールは、ブラック ホールの役割を果たします。

トラフィック転送インターフェイスをネットワーク内のスイッチの SPAN ポートに接続します。

トラフィック転送インターフェイス コンフィギュレーションには次の制限があります。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。
- ASA はシングル コンテキスト トランスペアレント モードである必要があります。
- トラフィック転送インターフェイスは、VLAN または BVI ではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられた VLAN を設定することはできません。
- トラフィック転送インターフェイスは、ASA トラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含む ASA 機能向けに設定したりすることはできません。

例

次の例は、GigabitEthernet 0/5 をトラフィック転送インターフェイスとして設定します。

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。
cxsc	トラフィックを ASA CX モジュールにリダイレクトするサービス ポリシー コマンド。
sfr	トラフィックを ASA FirePOWER モジュールにリダイレクトするサービス ポリシー コマンド。

traffic-non-sip

既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可するには、パラメータ コンフィギュレーション モードで **traffic-non-sip** 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。

traffic-non-sip

no traffic-non-sip

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

このコマンドは、デフォルトでイネ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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# traffic-non-sip
```

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。

transfer-encoding

転送エンコーディング タイプを指定して HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセス可能な HTTP マップ コンフィギュレーション モードで、**transfer-encoding** 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。

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

アクション	指定した転送エンコーディング タイプを使用する接続が検出されたときに実行するアクションを指定します。
allow	メッセージを許可します。
chunked	メッセージ本文を一連のチャンクとして転送する転送エンコーディング タイプを識別します。
compress	メッセージ本文を UNIX ファイル圧縮を使用して転送する転送エンコーディング タイプを識別します。
デフォルト	トラフィックが設定されたリストにないサポートされる要求方式を含む場合に ASA が実行するデフォルトのアクションを指定します。
deflate	メッセージ本文を zlib 形式（RFC 1950）とデフレート圧縮（RFC 1951）を使用して転送する転送エンコーディング タイプを識別します。
drop	接続を閉じます。
gzip	メッセージ本文を GNU zip（RFC 1952）を使用して転送する転送エンコーディング タイプを識別します。
identity	転送エンコーディングが実行されていないメッセージ本文の接続を識別します。
ログ	（任意）syslog を生成します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。
type	HTTP アプリケーション インスペクションを通じて制御される転送エンコーディングのタイプを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。コマンドがイネーブルで、サポートされる転送エンコーディング タイプが指定されていない場合、デフォルト アクションでは、ロギングなしで接続を許可します。デフォルトのアクションを変更するには、**default** キーワードを使用して、別のデフォルト アクションを指定します。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

transfer-encoding コマンドがイネーブルの場合、ASA は、サポートされ設定されている各転送エンコーディング タイプの HTTP 接続に指定されたアクションを適用します。

ASA は、設定されたリストの転送エンコーディング タイプに一致*しない*すべてのトラフィックに**デフォルト**のアクションを適用します。設定済みの**デフォルト**のアクションでは、ロギングなしで接続を**許可**します。

たとえば、設定済みのデフォルトのアクションでは、**drop** と **log** のアクションを伴う 1 つ以上のエンコーディング タイプを指定した場合、ASA は、設定されたエンコーディング タイプを含む接続をドロップし、各接続をロギングし、その他のサポートされるエンコーディング タイプの接続をすべて許可します。

より限定的なポリシーを設定する場合は、デフォルトのアクションを **drop**（または **reset**）と **log**（イベントをロギングする場合）に変更します。その後、許可されたエンコーディング タイプそれぞれに **allow** アクションを設定します。

適用する各設定に対して 1 回ずつ **transfer-encoding** コマンドを入力します。デフォルト アクションを変更するために **transfer-encoding** コマンドの 1 つのインスタンスを使用し、設定された転送エンコーディング タイプのリストに各エンコーディング タイプを追加するために 1 つのインスタンスを使用します。

設定されたアプリケーション タイプのリストからアプリケーション カテゴリを削除するために、このコマンドの **no** 形式を使用する場合は、コマンドラインのアプリケーション カテゴリ キーワードの後ろの文字は無視されます。

例

次に、特に禁止されていないすべてのサポートされるアプリケーション タイプを許可する設定済みのデフォルトを使用して、許可ポリシーを提供する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# transfer-encoding gzip drop log
ciscoasa(config-http-map)#
```

この場合、GNU zip を使用する接続だけがドロップされ、そのイベントがロギングされます。

次に、デフォルト アクションを、接続のリセットと、特に許可されていないすべてのエンコーディング タイプのロギングに変更した、限定的なポリシーを提供する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# port-misuse default action reset log
ciscoasa(config-http-map)# port-misuse identity allow
ciscoasa(config-http-map)#
```

この場合、転送エンコーディングを使用していない接続だけが許可されます。他のサポートされるエンコーディング タイプの HTTP トラフィックを受信した場合は、ASA は接続をリセットして syslog エントリを作成します。

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。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
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。

trustpoint（saml idp）

IDP 認証または SP 認証の証明書を含むトラストポイントを設定するには、SAML IDP コンフィギュレーション モードで **trustpoint** コマンドを使用します。SAML IDP コンフィギュレーション モードにアクセスするには、まず **webvpn** コマンドを入力します。トラストポイントを削除するには、このコマンドの **no** 形式を使用します。

trustpoint {**idp** | **sp**} *trustpoint-name*

no trustpoint {**idp** | **sp**} *trustpoint-name*

構文の説明

trustpoint-name	使用するトラストポイントの名前を指定します。
sp	トラストポイントには、ASA の署名を確認したり SAML アサーションを暗号化するための IdP の ASA（SP）証明書が含まれます。
idp	トラストポイントには、SAML アサーションを確認するための ASA の IdP 証明書が含まれます。

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	トランスペアレント	シングル	コンテキスト	システム
SAML IDP コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。

関連コマンド

コマンド	説明
saml idp	サードパーティ製 IdP の設定を作成し、SAML 属性を設定できるように SAML IDP モードを開始します。

trustpoint（SSO サーバ）（非推奨）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントの名前を指定するには、SSO サーバ モードで **trustpoint** コマンドを使用します。トラストポイント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。

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

構文の説明

trustpoint-name	使用するトラストポイン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	トランスペアレント	シングル	コンテキスト	システム
config-webvpn-sso-saml	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されます。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

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。ASA は現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。

例

次に、config-webvpn-sso-saml モードを開始し、SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントに名前を付ける例を示します。

```
ciscoasa(config-webvpn)# sso server
ciscoasa(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント情報を管理します。
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	SSO サーバのタイプを作成、命名、および指定します。

trust-verification-server

HTTPS の確立時に Cisco Unified IP Phones でのアプリケーション サーバの認証を可能にする信頼検証サービス サーバを指定するには、SIP インスペクションのパラメータ コンフィギュレーション モードで **trust-verification-server** 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。

trust-verification-server {**ip** *address* | **port** *number*}

no trust-verification-server {**ip** *address* | **port** *number*}

構文の説明

ip *address*	信頼検証サービス サーバの IP アドレスを指定します。SIP インスペクション ポリシー マップでこの引数を指定してこのコマンドを入力できるのは 4 回までです。SIP インスペクションは、登録された電話機ごとに各サーバへのピンホールを開き、電話機はどのサーバを使用するかを決定します。Cisco Unified Communications Manager（CUCM）サーバで、信頼検証サービス サーバを設定します。
port *number*	サーバが使用するポート番号を指定します。使用できるポート範囲は 1026 ～ 32768 です。

デフォルト

デフォルト ポートは 2445 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで 4 つの信頼検証サービス サーバを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.1
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.2
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.3
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.4
ciscoasa(config-pmap-p)# trust-verification-server port 2445
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション 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。

tsig enforced

TSIG リソース レコードの存在を必須とするには、パラメータ コンフィギュレーション モードで **tsig enforced** 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。

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

構文の説明

drop	TSIG が存在しない場合にパケットをドロップします。
ログ	システム メッセージ ログを生成します。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DNS トランザクションにおける TSIG の存在のモニタと強制をイネーブルにします。

例

次に、DNS インスペクション ポリシー マップ内で TSIG 強制をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tsig enforced action 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。
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。

ttl-evasion-protection

存続可能時間（TTL）回避保護をイネーブルにするには、TCP マップ コンフィギュレーション モードで **ttl-evasion-protection** 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。

ttl-evasion-protection

no ttl-evasion-protection

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

提供される TTL 回避保護は、デフォルトでイネーブルです。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用して、セキュリティ ポリシーを回避しようとする攻撃を阻止できます。TTL 回避保護により、接続の最大 TTL は最初のパケットの TTL によって決定します。後続パケットの TTL は削減できますが、増やすことはできません。システムは、TTL をその接続の以前の最小 TTL にリセットします。

たとえば、攻撃者は非常に短い TTL を持ち、ポリシーに合致するパケットを送信できます。TTL がゼロになると、ASA とエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、ASA にとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。この機能をイネーブルにすると、このような攻撃を阻止します。

例

次に、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローに対して TTL 回避保護をディセーブルにする例を示します。

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# no ttl-evasion-protection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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。

tunnel destination

VTI トンネルの宛先の IP アドレスを指定するには、インターフェイス コンフィギュレーション モードで **tunnel destination** コマンドを使用します。VTI トンネルの宛先 IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

tunnel destination {*IP address* | *hostname*}

no tunnel destination {*IP address* | *hostname*}

構文の説明

IP address	VTI トンネルの宛先の IP アドレス（IPv4）を指定します。
hostname	VTI トンネルの宛先のホスト名を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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	トランスペアレント	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	• あり	• なし	• あり	• なし	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。

例

次の例では、VTI トンネルの宛先の IP アドレスを指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel destination 10.2.2.3
```

関連コマンド

コマンド	説明
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。
tunnel protection ipsec	トンネル保護に使用される IPsec プロファイルを指定します。

トンネル モード

VTI トンネルにトンネル保護モードを指定するには、**tunnel mode** コマンドをインターフェイス コンフィギュレーション モードで使用します。VTI トンネル保護を削除するには、このコマンドの **no** 形式を使用します。

tunnel mode *ipsec IPv4*

no tunnel mode *ipsec IPv4*

構文の説明

ipsec	トンネル保護基準としてトンネルが IPsec を使用することを指定します。
IPv4	トンネルが IPsec over IPv4 を使用することを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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	トランスペアレント	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	• あり	• なし	• あり	• なし	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。

例

次の例では、保護モードとして IPsec を指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel mode ipsec ipv4
```

関連コマンド

コマンド	説明
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
tunnel protection ipsec	トンネル保護に使用される IPsec プロファイルを指定します。

tunnel protection ipsec

VTI トンネルに IPsec プロファイルを指定するには、**tunnel protection ipsec** コマンドをインターフェイス コンフィギュレーション モードで使用します。トンネルから IPsec プロファイルを削除するには、このコマンドの **no** 形式を使用します。

tunnel protection ipsec *IPsec profile name*

no tunnel protection ipsec *IPsec profile name*

構文の説明

ipsec profile name　使用する IPsec プロ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

次の表は、このコマンドを入力できるモードを示しています。

	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	トランスペアレント	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	• あり	• なし	• あり	• なし	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。このコマンドを使用すると、IKEv1 ポリシーが IPsec プロファイルに接続されます。

例

次の例では、profile12 が IPsec プロファイルです。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec profile12
```

関連コマンド

コマンド	説明
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。

tunnel source interface

VTI トンネルに送信元インターフェイスを指定するには、**tunnel source interface** コマンドをインターフェイス コンフィギュレーション モードで使用します。VTI トンネルの送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

tunnel source interface *interface name*

no tunnel source interface *interface name*

構文の説明

interface name	VTI トンネルを作成するために使用される送信元インターフェイスを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	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	トランスペアレント	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	• あり	• なし	• あり	• なし	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用した後、インターフェイス コンフィギュレーション モードで使用できます。IP アドレスは、選択されたインターフェイスから取得されます。

例

次の例では、VTI トンネルの送信元インターフェイスを指定します。

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel source interface outside
```

関連コマンド

コマンド	説明
interface tunnel	新しい VTI トンネル インターフェイスを作成します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。
tunnel protection ipsec	トンネル保護に使用される IPsec プロファイルを指定します。

tunnel-group

IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成し管理するには、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを使用します。トンネル グループを削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **type** *type*

no tunnel-group *name*

構文の説明

name	トンネル グループの名前を指定します。任意のストリングを選択できます。名前が IP アドレスの場合は、通常、ピアの IP アドレスとなります。
type	トンネル グループのタイプを指定します。 • remote-access：ユーザに IPsec リモート アクセスまたは WebVPN（ポータルまたはトンネル クライアント）のいずれかを使用した接続を許可します。 • ipsec-l2l：2 つのサイトまたは LAN がインターネットなどのパブリック ネットワークを介してセキュアに接続できる IPsec LAN-to-LAN を指定します。 （注） 次のトンネル グループ タイプは、リリース 8.0(2) で廃止されました。 ipsec-ra：IPsec リモート アクセス webvpn：WebVPN ASA はこれらを remote-access タイプに変換します。

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	トランスペアレント	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	• 対応	「注」を参照してください。	• 対応	• 対応	—

(注) tunnel-group コマンドは、トランスペアレント ファイアウォール モードで使用可能です。このモードでは、LAN-to-LAN トンネル グループのコンフィギュレーションは設定できますが、remote-access グループまたは WebVPN グループの設定はできません。LAN-to-LAN に対応する **tunnel-group** コマンドはすべてトランスペアレント ファイアウォール モードで使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	webvpn タイプが追加されました。
8.0(2)	remote-access タイプが追加され、ipsec-ra タイプと webvpn タイプが廃止されました。
8.3(1)	*name* 引数は、IPv6 アドレスに対応するために、変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

SSL VPN ユーザ（AnyConnect およびクライアントレスの両方）は、次の各種方式を使用して、アクセスするトンネル グループを選択できます。

- group-url
- group-alias
- 証明書マップ（証明書を使用する場合）

このコマンドとサブコマンドによって、ユーザが webvpn サービスにログインするときにドロップダウン メニューでグループを選択できるように ASA を設定します。メニューに表示されるグループは、ASA で設定された実際の接続プロファイル（トンネル グループ）のエイリアスまたは URL です。

ASA には、次のデフォルト トンネル グループがあります。

- DefaultRAGroup、デフォルトの IPsec remote-access トンネル グループ
- DefaultL2LGroup、デフォルトの IPsec LAN-to-LAN トンネル グループ
- DefaultWEBVPNGroup、デフォルトの WebVPN トンネル グループ

これらのグループは変更できますが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

tunnel-group コマンドを入力した後、適切な後続のコマンドを入力して、特定のトンネル グループの特定の属性を設定できます。これらのコマンドはそれぞれ、トンネル グループ属性を設定するためのコンフィギュレーション モードを開始します。

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

LAN-to-LAN 接続に対して、ASA は、トンネル グループを、クリプト マップで設定されたピア アドレスを同名のトンネル グループと一致させることで、接続のためのトンネル グループの選択しようとします。そのため、IPv6 ピアに対し、その IPv6 のアドレスと同様にトンネル グループ名を設定する必要があります。トンネル グループ名は、短い表記または長い表記で設定できます。CLI を使うと、その名前を最短の表記にできます。たとえば、トンネル グループ コマンドを次のように入力した場合、

```
ciscoasa(config)# tunnel-group 2001:0db8:0000:0000:0000:0000:1428:57ab type ipsec-l2l
```

トンネル グループはコンフィギュレーションで次のように表示されます。

```
tunnel-group 2001:0db8::1428:57ab type ipsec-l2l
```

例

次に、グローバル 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。最初に、リモート アクセス トンネル グループを設定します。グループ名は group1 です。

```
ciscoasa(config)# tunnel-group group1 type remote-access
ciscoasa(config)#
```

次に、webvpn トンネル グループ「group1」を設定する tunnel-group コマンドの例を示します。このコマンドはグローバル コンフィギュレーション モードで入力します。

```
ciscoasa(config)# tunnel-group group1 type webvpn
ciscoasa(config)#
```

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。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	設定一般モードを開始し、全般的なトンネル グループ属性を設定します。
tunnel-group ipsec-attributes	設定 ipsec モードを開始し、IPsec トンネル グループ属性を設定します。
tunnel-group ppp-attributes	L2TP 接続の PPP 設定を行うための設定 ppp モードを開始します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

tunnel-group general-attributes

一般属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、すべてのサポートされるトンネリング プロトコルに共通の設定値を設定するために使用されます。

すべての一般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。

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

構文の説明

general-attributes	このトンネル グループの属性を指定します。
name	トンネル グループ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	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	他のトンネル グループ タイプのさまざまな属性が、一般トンネル グループ属性リストに移行され、トンネル グループ一般属性モードのプロンプトが変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用してリモート アクセス接続のリモート アクセス トンネル グループを作成し、その後、トンネル グループ一般属性を設定するための一般属性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。トンネル グループの名前は、209.165.200.225 です。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type remote-access
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
ciscoasa(config-tunnel-general)#
```

次に、グローバル コンフィギュレーション モードで、IPsec リモート アクセス接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の一般属性を設定するための一般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。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group ipsec-attributes

ipsec 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group ipsec-attributes** コマンドを使用します。このモードは、IPsec トンネリング プロトコルに固有の設定値を設定するために使用されます。

すべての IPsec 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。

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

構文の説明

ipsec-attributes	このトンネル グループの属性を指定します。
name	トンネル グループ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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	さまざまな IPsec トンネル グループ属性が一般トンネル グループ属性リストに移行され、トンネル グループ ipsec 属性モードのプロンプトが変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードで、IPsec リモート アクセス トンネル グループ remotegrp のトンネル グループを作成し、その後、IPsec グループ属性を指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group-list enable

tunnel-group group-alias で定義されているトンネル グループをイネーブルにするには、**tunnel-group-list enable** コマンドを使用します。

tunnel-group-list enable

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

このコマンドは、クライアントレスまたは AnyConnect VPN クライアント セッションで tunnel-group group-alias および group-url コマンドと組み合わせて使用します。このコマンドは、ログイン ページに tunnel-group ドロップダウンが表示されるように機能をイネーブルにします。group-alias は、エンド ユーザに表示するために ASA 管理者が定義した、従業員、技術部門、コンサルタントなどのテキスト文字列です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)# group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
```

関連コマンド

コマンド	説明
tunnel-group	VPN 接続プロファイルを作成するか、または VPN 接続プロファイルのデータベースにアクセスします。
group-alias	接続プロファイル(トンネル グループ)のエイリアスを設定します。
group-url	VPN エンドポイントで指定されている URL または IP アドレスと接続プロファイルを照合します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

tunnel-group-map

適応型セキュリティ アプライアンスが IPSec 接続要求をクライアント証明書認証とともに受信すると、設定したポリシーに従って接続プロファイルをその接続に割り当てます。

そのポリシーは、設定したルールの使用、証明書の OU フィールドの使用、IKE ID（ホスト名、IP アドレス、キー ID など）の使用、クライアントの IP アドレス、あるいは接続プロファイルを割り当てるデフォルトの接続プロファイルになります。SSL 接続に対し、適応型セキュリティ アプライアンスは、接続プロファイルを割り当てるように設定したルールを使用するだけです。

既存のマップ名を接続プロファイルに関連付けて設定したルールに基づき、**tunnel-group-map** コマンドにより、接続プロファイルが接続に割り当てられます。

接続プロファイルとマップ名の関連を解消するには、このコマンドの **no** 形式を使用します。このコマンドの no 形式ではマップ名は削除されません。マップ名と接続プロファイルとの関連が解消されるだけです。

コマンドの構文は次のとおりです。

tunnel-group-map [mapname] [rule-index] [connection-profile]

no tunnel-group-map [mapname] [rule-index]

(注)
- このコマンドで証明書マップ名を作成できます。
  crypto ca certificate map [mapname] [rule-index]
- 「トンネル グループ」は、現在「接続プロファイル」と呼ばれている用語の旧称です。tunnel-group-map コマンドは、接続プロファイル マップを作成するものと考えてください。

構文の説明

mapname	必須です。既存の証明書マップの名前を指定します。
rule-index	必須です。マップ名に関連付けられた rule-index を指定します。rule-index パラメータは、**crypto ca certificate map** コマンドを使用して定義されます。有効な値は 1 ～ 65535 です。
connection-profile	証明書マップ リストに対して接続プロファイル名を指定します。

デフォルト

tunnel-group-map が未定義で、ASA が IPsec 接続リストをクライアント証明書認証とともに受信した場合、ASA は証明書認証要求をこれらのポリシーの 1 つと次の順序で照合することで、接続プロファイルを割り当てます。

証明書の ou フィールド：サブジェクト Distinguish Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）フィールドの値に基づき、接続プロファイルを決定します。

IKE ID：フェーズ 1 IKE ID の内容に基づき、接続プロファイルを決定します。

peer-ip：確立されたクライアント IP アドレスに基づき、接続プロファイルを決定します。

デフォルト接続プロファイル：ASA が上記 3 つのポリシーに一致しない場合は、デフォルトの接続プロファイルを割り当てます。デフォルトのプロファイルは DefaultRAGroup です。そうでない場合は、デフォルトの接続プロファイルは、tunnel-group-map default-group コマンドを使用して設定されます。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

設定したマップ名は、接続プロファイルと関連付ける前に、存在している必要があります。**crypto ca certificate map** コマンドを使用して、マップ名を作成します。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

マップ名を接続プロファイルに関連付けたら、前述のデフォルトのポリシーではなく設定したルールを使用するには、tunnel-group-map をイネーブルにする必要があります。これを行うには、グローバル コンフィギュレーション モードで **tunnel-group-map enable rules** コマンドを実行する必要があります。

例

次の例では、rule index が **10** のマップ名 **SalesGroup** を **SalesConnectionProfile** 接続プロファイルに関連付けています。

```
ciscoasa(config)# tunnel-group-map SalesGroup 10 SalesConnectionProfile
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map [map name]	CA 証明書マップ コンフィギュレーション モードを開始し、そのモードを使用して証明書マップ名を作成できます。
tunnel-group-map enable	確立されたルールに基づく証明書ベースの IKE セッションをイネーブルにします。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルトのトンネル グループとして指定します。

tunnel-group-map default-group

tunnel-group-map default-group コマンドでは、他の設定された方式を使用して名前を判別できない場合に使用するデフォルトのトンネル グループを指定します。

tunnel-group-map を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

構文の説明

default-group *tunnel-group-name*	他の設定された方式では名前を取得できない場合に使用するデフォルトのトンネル グループを指定します。*tunnel-group name* はすでに存在している必要があります。
rule index	オプション。**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map default-group のデフォルト値は DefaultRAGroup 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ ルールもこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は group1 です。

```
ciscoasa(config)# tunnel-group-map default-group group1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	クリプト CA 証明書マップ コンフィギュレーション モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。

tunnel-group-map enable

tunnel-group-map enable コマンドでは、証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。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。

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

構文の説明

ポリシー	証明書からトンネル グループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。 **ike-id**：トンネル グループがルール ルックアップに基づいて判別されない、または ou から取得されない場合は、フェーズ 1 IKE ID の内容に基づいて証明書ベースの IKE セッションをトンネル グループにマッピングされることを示します。 **ou**：トンネル グループがルール ルックアップに基づいて判別されない場合は、サブジェクト認定者名（DN）の組織ユニット（OU）の値が使用されることを示します。 **peer-ip**：トンネル グループが規則の検索に基づいて決定されないか、ou または ike-id 方式から取得されない場合、確立されたピア IP アドレスを使用することを示します。 **rules**：このコマンドによって設定された証明書マップ アソシエーションに基づいて、証明書ベースの IKE セッションがトンネル グループにマッピングされることを示します。
rule index	（任意）**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map コマンドのデフォルト値は **enable ou** で、**default-group** は DefaultRAGroup に設定されています。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

例

次に、フェーズ 1 IKE ID の内容に基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable ike-id
ciscoasa(config)#
```

次に、確立済みのピアの IP アドレスに基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable peer-ip
ciscoasa(config)#
```

次に、サブジェクト認定者名（DN）の組織ユニット（OU）に基づく、証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable ou
ciscoasa(config)#
```

次に、確立済みのルールに基づく証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group-map enable rules
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルトのトンネル グループとして指定します。

tunnel-group ppp-attributes

ppp 属性コンフィギュレーション モードを開始し、IPsec を介した L2TP 接続によって使用される PPP 設定値を設定するには、グローバル コンフィギュレーション モードで **tunnel-group ppp-attributes** コマンドを使用します。

すべての PPP 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。

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

構文の説明

name	トンネル グループ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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

PPP 設定値はレイヤ 2 トンネリング プロトコル（L2TP）によって使用されます。L2TP は、リモート クライアントがダイヤルアップ電話サービスのパブリック IP ネットワークを使用してプライベート社内ネットワーク サーバとセキュアに通信できるようにする VPN トンネリング プロトコルです。L2TP はクライアント/サーバ モデルに基づき、PPP over UDP（ポート 1701）を使用してデータをトンネルします。tunnel-group ppp コマンドはすべて、PPPoE トンネル グループ タイプで使用できます。

例

次に、トンネル グループ *telecommuters* を作成し、ppp 属性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。

```
ciscoasa(config)# tunnel-group telecommuters type pppoe
ciscoasa(config)# tunnel-group telecommuters ppp-attributes
ciscoasa(tunnel-group-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group-preference

エンドポイントで指定された URL と一致するグループ URL を含む接続プロファイルに VPN プリファレンスを変更するには、webvpn コンフィギュレーション モードで **tunnel-group-preference** 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、**no** 形式を使用します。

tunnel-group-preference group-url

no tunnel-group-preference group-url

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。

コマンド デフォルト

デフォルトでは、接続プロファイルで指定された証明書のフィールド値とエンドポイントで使用される証明書のフィールド値が ASA によって照合され、一致した場合は、そのプロファイルが VPN 接続に割り当てられます。このコマンドは、デフォルトの動作を上書きします。

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	トランスペアレント	シングル	コンテキスト	システム
config-webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(5)/8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、接続プロファイルの選択プロセス中に、接続プロファイルのプリファレンスを変更します。これにより、ASA ソフトウェアの数多くの旧リリースによって使用されるグループ URL プリファレンスを利用できます。エンドポイントによって、接続プロファイルにないグループ URL が指定され、かつ接続プロファイルの証明書値と一致する証明書値が指定されている場合、ASA ではその接続プロファイルを VPN セッションに割り当てます。

このコマンドは webvpn コンフィギュレーション モードで入力しますが、このコマンドによって、ASA によってネゴシエートされたすべてのクライアントレスおよび AnyConnect VPN 接続について、接続プロファイルの選択プリファレンスが変更されます。

例

次に、接続プロファイルの選択プロセス中に、接続プロファイルのプリファレンスを変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-preference group-url
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
tunnel-group	VPN 接続プロファイルを作成するか、または VPN 接続プロファイルのデータベースにアクセスします。
group-url	VPN エンドポイントで指定されている URL または IP アドレスと接続プロファイルを照合します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

tunnel-group webvpn-attributes

webvpn 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードでは、WebVPN トンネリングに共通の設定値を設定します。

すべての WebVPN 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。

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

構文の説明

name	トンネル グループの名前を指定します。
webvpn-attributes	このトンネル グループの WebVPN 属性を指定します。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.8(1)	pre-fill-username および secondary-pre-fill-username の値が clientless から client に変更されました。

使用上のガイドライン

一般属性に加えて、webvpn 属性モードで WebVPN 接続に固有の次の属性も設定できます。

- authentication
- customization
- dns-group
- group-alias
- group-url
- without-csd

pre-fill-username および secondary-pre-fill-username 属性は、認証および認可に使用する証明書からユーザ名を抽出するために使用されます。値は client または clientless です。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用して WebVPN 接続用のトンネル グループを作成し、その後、WebVPN 属性を設定するための webvpn 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。トンネル グループの名前は、209.165.200.225 です。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type webvpn
ciscoasa(config)# tunnel-group 209.165.200.225 webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

次に、グローバル コンフィギュレーション モードで、WebVPN 接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の WebVPN 属性を設定するための webvpn 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。

```
ciscoasa(config)# tunnel-group remotegrp type webvpn
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-limit

許可されるアクティブな GTP トンネルの最大数を指定するには、ポリシー マップ パラメータ コンフィギュレーション モードで **tunnel limit** コマンドを使用します。トンネル制限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。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

構文の説明

max_tunnels	許可されるトンネルの最大数。これは、PDP コンテキストまたはエンドポイントの数に相当します。

デフォルト

デフォルトのトンネル制限値は 500 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。

例

次に、GTP トラフィックの最大トンネル数を 10,000 に指定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 10000
```

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。
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。

tx-ring-limit

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 **tx-ring-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。

(注) このコマンドは ASA 5580 10 ギガビット イーサネット インターフェイス、ASA 5512-X ～ ASA 5555-X 管理インターフェイス、または ASA サービス モジュールではサポートされません（10 ギガビット イーサネット インターフェイスは、ASA 5585-X のプライオリティ キューに対してサポートされます）。

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

構文の説明

number-of-packets	イーサネット送信ドライバが許容できる低遅延パケットまたは標準のプライオリティのパケットの最大数を指定します。このパケットの処理が終わると、イーサネット送信ドライバは輻輳が解消するまで、インターフェイス上のパケットをバッファしているキューの処理に戻ります。指定できる範囲は 3 ～ 511 です。

デフォルト

デフォルト値は 511 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	トランスペアレント	シングル	コンテキスト	システム
プライオリティ キュー	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA 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）用の低遅延キューイング（LLQ）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。ASA 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いずれかのタイプ（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。

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。

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。

例

次の例では、test というインターフェイスにプライオリティ キューを、キュー制限を 2048 パケットに、送信キュー制限を 256 パケットに設定しています。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 2048
ciscoasa(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。
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。

コマンド	説明
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。
show running-config 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** キーワードを指定した場合、このコマンドは、現在の **priority-queue**、**queue-limit**、および **tx-ring-limit** コマンドのコンフィギュレーション値をすべて表示します。

type echo

SLA 動作をエコー応答時間プローブ動作として設定するには、SLA モニタ コンフィギュレーション モードで **type echo** コマンドを使用します。SLA コンフィギュレーションからタイプを削除するには、このコマンドの **no** 形式を使用します。

type echo protocol ipIcmpEcho *target* **interface** *if-name*

no type echoprotocol ipIcmpEcho *target* **interface** *if-name*

構文の説明

interface *if-name*	エコー要求パケットを送信するために使用されるインターフェイスのインターフェイス名を、**nameif** コマンドで指定されているとおりに指定します。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。
protocol	プロトコルのキーワード。サポートされる唯一の値が **ipIcmpEcho** で、エコー動作で IP/ICMP エコー要求を使用するように指定します。
target	モニタするオブジェクトの IP アドレスまたはホスト名。

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	トランスペアレント	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ICMP パケットのペイロードのデフォルト サイズは 28 バイトで、合計サイズが 64 バイトの ICMP パケットを作成します。ペイロード サイズは、**request-data-size** コマンドを使用して変更できます。

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。SLA の到達可能性を追跡するために、ID が 1 のトラッキング エントリを作成します。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(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。
request-data-size	SLA 動作要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。

uc-ime コマンド～ username-prompt コマンド

uc-ime（非推奨）

Cisco Intercompany Media Engine プロキシ インスタンスを作成するには、グローバル コンフィギュレーション モードで **uc-ime** コマンドを使用します。このプロキシ インスタンスを削除するには、このコマンドの **no** 形式を使用します。

uc-ime *uc-ime_name*

no uc-ime *uc-ime_name*

構文の説明

uc-ime_name	ASA 上で設定されている Cisco Intercompany Media Engine プロキシのインスタンス名を指定します。*name* は 64 文字までに制限されています。 ASA に設定できる Cisco Intercompany Media Engine プロキシは 1 つだけです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine プロキシを設定します。Cisco Intercompany Media Engine により、企業はインターネット経由での相互接続をオンデマンドで行うことが可能になり、VoIP テクノロジーによる高度な機能を利用できます。Cisco Intercompany Media Engine では、ピアツーピア、セキュリティ、および SIP プロトコルを使用してビジネス間にダイナミック SIP トランクを作成することにより、異なる企業内の Cisco Unified Communications Manager クラスタの間で企業間フェデレーションを実現できます。企業の集合は、最終的にそれらの間にクラスタ間トランクが存在する 1 つの大きなビジネスであるかのように連携します。

メディア ターミネーション インスタンスは、Cisco Intercompany Media Engine プロキシで指定する前に作成する必要があります。

ASA に設定できる Cisco Intercompany Media Engine プロキシは 1 つだけです。

例

次に、**uc-ime** コマンドを使用して Cisco Intercompany Media Engine プロキシを設定する例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

関連コマンド

コマンド	説明
fallback	接続の整合性が低下する場合に VoIP から PSTN へのフォールバックに Cisco Intercompany Media Engine が使用するフォールバック タイマーを設定します。
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
ticket	Cisco Intercompany Media Engine プロキシのチケット エポックおよびパスワードを設定します。
ucm	Cisco Intercompany Media Engine プロキシの接続先の Cisco UCM を設定します。

ucm（廃止）

Cisco Intercompany Media Engine プロキシの接続先の Cisco Unified Communications Manager（UCM）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 **ucm** コマンドを使用します。Cisco Intercompanuy Media Engine プロキシに接続されている Cisco UCMs を削除するには、このコマンドの **no** 形式を使用します。

ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

no ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

構文の説明

address	Cisco Unified Communications Manager（UCM）の IP アドレスを設定するキーワードです。
ip_address	Cisco UCM の IP アドレスを指定します。IP アドレスは IPv4 形式で入力します。
nonsecure	Cisco UCM クラスタまたは Cisco UCM クラスタが非セキュア モードで動作するように指定します。
secure	Cisco UCM クラスタまたは Cisco UCM クラスタがセキュア モードで動作するように指定します。
trunk-security-mode	Cisco UCM クラスタまたは Cisco UCM クラスタのセキュリティ モードを設定するキーワードです。

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	トランスペアレント	シングル	コンテキスト	システム
UC-IME コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

企業内の Cisco UCM サーバを指定します。

Cisco Intercompany Media Engine プロキシの **ucm** コマンドを複数入力できます。

(注) Cisco Intercompany Media Engine の SIP トランクがイネーブルになっているクラスタ内の各 Cisco UCM に対してエントリを追加する必要があります。

Cisco UCM または Cisco UCM に **secure** を指定することは、Cisco UCM または Cisco UCM クラスタが TLS を開始することを意味します。したがって、コンポーネントに TLS を設定する必要があります。

secure オプションは、この作業で設定することも、後で企業の TLS を設定するときに更新することもできます。

企業内の TLS は、ASA から見た Cisco Intercompany Media Engine トランクのセキュリティ ステータスを参照します。

Cisco UCM で Cisco Intercompany Media Engine トランクの転送セキュリティを変更する場合は、適応型セキュリティ アプライアンスでも変更する必要があります。一致していないと、コールは失敗します。適応型セキュリティ アプライアンスは、非セキュア IME トランクを持つ SRTP をサポートしません。適応型セキュリティ アプライアンスは、SRTP がセキュア トランクで許可されることを前提としています。したがって、TLS が使用される場合は、IME トランクに対して [SRTP Allowed] をオンにする必要があります。ASA は、セキュア IME トランク コールに対して SRTP から RTP へのフォールバックをサポートしています。

プロキシは企業のエッジに置かれ、企業間で作成される SIP トランク間の SIP シグナリングを検査します。プロキシはインターネットから TLS シグナリングを終端し、TCP または TLS を Cisco UCM に対して開始します。

Transport Layer Security（TLS）は、インターネットなどのネットワーク経由の通信にセキュリティを提供する暗号化プロトコルです。TLS によって、トランスポート層エンドツーエンドでのネットワーク接続のセグメントが暗号化されます。

この作業は、内部ネットワーク内で TCP が許可されている場合は必要ありません。

ローカルの企業内で TLS を設定するための主要な手順を次に示します。

- ローカルの ASA で、自己署名証明書の別の RSA キーおよびトラストポイントを作成します。
- ローカル Cisco UCM とローカルの ASA 間で証明書をエクスポートおよびインポートします。
- ASA でローカル Cisco UCM のトラストポイントを作成します。

TLS を介した認証：N 社の企業のために ASA がポートとして機能するためには、Cisco UCM は ASA からの証明書の受け入れを許可する必要があります。この処理は、Cisco UCM が証明書からサブジェクト名を抽出してセキュリティ プロファイルで設定されている名前と比較するため、ASA によって示されるサブジェクト名と同じものが含まれている同じ SIP セキュリティ プロファイルにすべての UC IME SIP トランクを関連付けることによって実行できます。

例

次に、UCM プロキシに接続する例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

包括的

DNS インスペクション エンジンが DNS ルックアップ要求を Cisco Umbrella へリダイレクトできるようにするには、DNS インスペクション ポリシーマップ パラメータ コンフィギュレーション モードで **umbrella** コマンドを使用します。Cisco Umbrella 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。

umbrella [**tag** *umbrella_policy*] [**fail-open**]

no umbrella [**tag** *umbrella_policy*] [**fail-open**]

構文の説明

fail-open	Cisco Umbrella DNS サーバが使用できない場合は、このポリシーマップで Umbrella に自身を無効にさせて、DNS 要求をシステムに設定されている他の DNS サーバ（ある場合）に移動できるようにします。Umbrella DNS サーバが再度使用可能になると、ポリシーマップはそれらの使用を再開します。 このオプションが含まれていない場合、DNS 要求は到達不能の Umbrella リゾルバへ移動し続けるので、応答は取得されません。
tag *umbrella_policy*	（任意）Cisco Umbrella に定義され、デバイスに適用される、エンタープライズ セキュリティ ポリシーの名前。ポリシーを指定しない場合、または入力した名前が Cisco Umbrella に存在しない場合、デフォルトのポリシーが指定されます。

デフォルト

タグを指定しないと、デバイス登録は、デフォルトのエンタープライズ セキュリティ ポリシーを指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。
9.12(1)	**fail-open** キーワードが追加されました。

使用上のガイドライン

DNS インスペクション ポリシーマップを設定する際に、次のコマンドを使用します。

アクティブな DNS インスペクション ポリシーマップのこのコマンドのプレゼンスは、Cisco Umbrella 登録サーバの登録プロセスを開始します。HTTPS 経由で行われる登録と接続を確立するには、登録サーバの CA 証明書をインストールしておく必要があります。

グローバル コンフィギュレーション モードで **umbrella-global** コマンド使用して、グローバル パラメータを設定する必要もあります。

例

次の例では、デフォルト ポリシーを使用して Umbrella を有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

次の例では、デフォルト ポリシーを使用して Umbrella のフェール オープンを有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。タグをすでに登録していて、**fail-open** オプションのみを追加する場合は、コマンドに同じタグを含める必要があります。そうしない場合、タグなしでデバイスを再登録することになります。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

umbrella-global

Cisco Umbrella ポータルにデバイスを接続するために必要なグローバル設定を設定するために、Umbrella コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **umbrella-global** コマンドを使用します。グローバル Umbrella コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

umbrella-global

no umbrella-global

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

デフォルトのグローバル Umbrella コンフィギュレーションはありません。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Umbrella サービスに登録する場合は、デバイスを Cisco Umbrella に登録するように設定できます。

Umbrella グローバル設定は、主に、Cisco Umbrella にデバイスを登録するために必要な API トークンを定義します。Cisco Umbrella ダッシュボードからトークンを取得します。

グローバル設定が Umbrella を有効にするために十分ではありません。パラメータ コンフィギュレーション モードで umbrella コマンドを使用して、DNS インスペクション ポリシーマップで Umbrella を有効にする必要もあります。

例

次の例では、グローバル Umbrella 設定を構成し、デフォルトの DNS インスペクション ポリシーマップで Umbrella を有効にする方法についても説明します。

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
local-domain-bypass	DNS 要求が Cisco Umbrella をバイパスする必要があるローカル ドメインを設定します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
resolver	DNS 要求を解決する Cisco Umbrella DNS サーバのアドレスを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella	DNS インスペクション エンジンで、DNS ルックアップ要求を Cisco Umbrella にリダイレクトできるようにします。

undebug

現在のセッションでデバッグ情報の表示をディセーブルにするには、特権 EXEC モードで **undebug** コマンドを使用します。

undebug {*command* | **all**}

構文の説明

all	すべてのデバッグ出力をディセーブルにします。
command	指定したコマンドのデバッグをディセーブルにします。サポートされるコマンドの詳細については、「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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

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ました。**debug** キーワードが追加されました。

使用上のガイドライン

次のコマンドは、**undebug** コマンドで使用できます。特定のコマンドのデバッグ、または特定の **debug** コマンドに関連付けられた引数とキーワードの詳細については、**debug** コマンドのエントリを参照してください。

- aaa：AAA 情報
- acl：ACL 情報
- all：すべてのデバッグ
- appfw：アプリケーション ファイアウォール情報
- arp：NP オペレーションを含む ARP
- asdm：ASDM 情報
- auto-update：Auto-update 情報
- boot-mem：ブート メモリの計算と設定
- cifs：CIFS 情報
- cmgr：CMGR 情報

- context：コンテキスト情報
- cplane：CP 情報
- crypto：クリプト情報
- ctiqbe：CTIQBE 情報
- ctl-provider：CTL プロバイダーのデバッグ情報
- dap：DAP 情報
- dcerpc：DCERPC 情報
- ddns：ダイナミック DNS 情報
- dhcpc：DHCP クライアント情報
- dhcpd：DHCP サーバ情報
- dhcprelay：DHCP リレー情報
- disk：ディスク情報
- dns：DNS 情報
- eap：EAP 情報
- eigrp：EIGRP プロトコル情報
- email：電子メール情報
- entity：エンティティ MIB 情報
- eou：EAPoUDP 情報
- esmtp：ESMTP 情報
- fips：FIPS 140-2 情報
- fixup：フィックスアップ情報
- fover：フェールオーバー情報
- fsm：FSM 情報
- ftp：FTP 情報
- generic：その他の情報
- gtp：GTP 情報
- h323：H323 情報
- http：HTTP 情報
- icmp：ICMP 情報
- igmp：インターネット グループ管理プロトコル
- ils：LDAP 情報
- im：IM インスペクション情報
- imagemgr：Image Manager 情報
- inspect：デバッグ情報のインスペクション
- integrityfw：Integrity ファイアウォール情報
- ip：IP 情報
- ipsec-over-tcp：IPsec over TCP 情報
- IPSec-pass-thru：ipsec-pass-thru 情報のインスペクション

- ipv6：IPv6 情報
- iua-proxy：IUA プロキシ情報
- kerberos：KERBEROS 情報
- l2tp：L2TP 情報
- ldap：LDAP 情報
- mfib：マルチキャスト転送情報ベース
- mgcp：MGCP 情報
- module-boot：サービス モジュール ブート情報
- mrib：マルチキャスト ルーティング情報ベース
- nac-framework：NAC-FRAMEWORK 情報
- netbios-inspect：NETBIOS インスペクション情報
- npshim：NPSHIM 情報
- ntdomain：NT ドメイン情報
- ntp：NTP 情報
- ospf：OSPF 情報
- p2p：P2P インスペクション情報
- parser：パーサー情報
- pim：Protocol Independent Multicast
- pix：PIX 情報
- ppp：PPP 情報
- pppoe：PPPoE 情報
- pptp：PPTP 情報
- radius：RADIUS 情報
- redundant-interface：冗長インターフェイス情報
- rip：RIP 情報
- rtp：RTP 情報
- rtsp：RTSP 情報
- sdi：SDI 情報
- sequence：シーケンス番号の追加
- session-command：セッション コマンド情報
- sip：SIP 情報
- skinny：Skinny 情報
- sla：IP SLA モニタ デバッグ
- smtp-client：電子メール システムのログ メッセージ
- splitdns：スプリット DNS 情報
- sqlnet：SQLNET 情報
- ssh：SSH 情報
- sunrpc：SUNRPC 情報

- tacacs：TACACS 情報
- tcp：WebVPN の TCP
- tcp-map：TCP マップ情報
- timestamps：タイムスタンプの追加
- track：スタティック ルート トラッキング
- vlan-mapping：VLAN マッピング情報
- vpn-sessiondb：VPN セッション データベース情報
- vpnlb：VPN ロード バランシング情報
- wccp：WCCP 情報
- webvpn：WebVPN 情報
- xdmcp：XDMCP 情報
- xml：XML パーサー情報

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべてのデバッグ出力をディセーブルにする例を示します。

```
ciscoasa(config)# undebug all
```

関連コマンド

コマンド	説明
debug	選択したコマンドに関するデバッグ情報を表示します。

unit join-acceleration

クラスタ結合の高速化を有効にするには、クラスタ コンフィギュレーション モードで **unit joint-acceleration** 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。

unit join-acceleration

no unit join-acceleration

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。

コマンド デフォルト

このコマンドは、デフォルトでイネ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	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

スレーブ ユニットがマスター ユニットと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、マスターからスレーブには複製されません。

(注) 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。互換性のない設定を表示するには、**show cluster info unit-join-acceleration incompatible-config** コマンドを使用します。

例

次に、クラスタ結合の高速化を無効にする例を示します。

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no unit join-acceleration
```

関連コマンド

コマンド	説明
クラスタ	クラスタ コンフィギュレーション モードを開始します

unit parallel-join

Firepower 9300 シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認するには、クラスタ グループ コンフィギュレーション モードで **unit parallel-join** コマンドを使用します。並行参加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。

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

no unit parallel-join [*num_of_units* **max-bundle-delay** *max_delay_time*]

構文の説明

num_of_units	モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数(1 ～ 3)を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは *max_delay_time* の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3 のすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。
max-bundle-delay *max_delay_time*	最大遅延時間を分単位(0 ～ 30 分)で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。*num_of_units* を 1 に設定した場合、この値は 0 にする必要があります。*num_of_units* を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。 たとえば、*num_of_units* を 3、*max_delay_time* を 5 分に設定します。モジュール 1 が起動すると、その 5 分間のタイマーが開始されます。モジュール 2 が 2 分後に起動すると、その 5 分間のタイマーが開始されます。モジュール 3 が 1 分後に起動し、すべてのモジュールが 4 分符号でクラスタに参加します。モジュールはタイマーが完了するまで待機しません。モジュール 3 が起動しない場合、モジュール 1 は 5 分間タイマーの終了時にクラスタに参加し、モジュール 2 も参加します。モジュール 2 はタイマーがまだ 2 分残っていますが、タイマーが完了するまで待機しません。

コマンド デフォルト

この機能はデフォルトで無効に設定されています。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(1)	コマンドが追加されました。

使用上のガイドライン　他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

例　次の例では、モジュールの数を 2 に、最大遅延時間を 6 分に設定します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# unit parallel-join 2 max-bundle-delay 6
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ コンフィギュレーション モードを開始します。

unix-auth-gid

UNIX グループ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-gid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid *identifier*

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルトは 65534 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

文字列でネットワーク ファイル システム（NetFS）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX グループ ID を 4567 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 4567
```

関連コマンド

コマンド	説明
unix-auth-uid	UNIX ユーザ ID を設定します。

unix-auth-uid

UNIX ユーザ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-uid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid *identifier*

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルトは 65534 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

文字列でネットワーク ファイル システム（NetFS）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX ユーザ ID を 333 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 333
```

関連コマンド

コマンド	説明
unix-auth-gid	UNIX グループ ID を設定します。

unsupported

ソフトウェアで直接サポートされていない Diameter 要素をロギングするには、ポリシー マップ パラメータ コンフィギュレーション モードで **unsupported** コマンドを使用します。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。

unsupported {**application-id** | **avp** | **command-code**} **action log**

no unsupported {**application-id** | **avp** | **command-code**} **action log**

構文の説明

application-id	アプリケーション ID が直接サポートされていない Diameter メッセージをロギングします。
avp	直接サポートされていない属性値ペア（AVP）が含まれている Diameter メッセージをロギングします。
command-code	直接サポートされていないコマンド コードが含まれている Diameter メッセージをロギングします。

デフォルト

デフォルトでは、ロギングなしで要素が許可されています。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

Diameter インスペクション ポリシー マップを設定する場合に、このコマンドを使用します。

これらのオプションでは、ソフトウェアで直接サポートされていないアプリケーション ID、コマンド コード、および AVP が指定されます。デフォルトでは、ロギングなしで要素が許可されています。コマンドを 3 回入力して、すべての要素のロギングを有効にできます。

例

次に、サポートされていないすべてのアプリケーション ID、コマンド コード、および AVP をロギングする例を示します。

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# unsupported application-id action log
ciscoasa(config-pmap-p)# unsupported command-code action log
ciscoasa(config-pmap-p)# unsupported avp action log
```

関連コマンド

コマンド	説明
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

upgrade rommon

ASA 5506-X および ASA 5508-X シリーズ セキュリティ アプライアンスをアップグレードするには、特権 EXEC モードで **upgrade rommon** コマンドを使用します。

upgrade rommon [disk0 | disk1 | flash]:/[*path*] *filename*

構文の説明

disk0:/[*path*/]*filename*	このオプションは内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。
disk1:/[*path*/]*filename*	このオプションは外部フラッシュ メモリ カードを示します。
flash:/[*path*/]*filename*	このオプションは、内部フラッシュ カードを示します。**flash** は **disk0** のエイリアスです。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

コマンドにファイル名を指定すると、コマンドによってファイルが確認され、アップグレードを確認するよう求められます。設定情報を保存していない場合、リロードを開始する前に情報を保存するように促されます。確認すると、ASA は ROMMON になり、アップグレード手順が開始されます。

例

次に、ASA 5506-X および ASA 5508-X シリーズ セキュリティ アプライアンスをアップグレードする例を示します。

```
ciscoasa# upgrade rommon disk0:/kenton_rommon_1-0-19_release.SPA
Verifying file integrity of disk0:/kenton_rommon_1-0-19_release.SPA

Computed Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4
```

```
Embedded Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4


Digital signature successfully validated
File Name                     : disk0:/kenton_rommon_1-0-19_release.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54232BC5
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

upload-max-size

(注) **upload-max-size** コマンドは機能しません。使用しないでください。ただし、実行コンフィギュレーションでは表示される場合があり、CLI で使用できます。

アップロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **upload-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

upload-max-size *size*

no upload-max-size

構文の説明

size	アップロードされるオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル設定を設定できます。

srv-id

参照 ID オブジェクトに URI ID を設定するには、*ca-reference-identity* モードで **uri-id** コマンドを使用します。URI ID を削除するには、このコマンドの **no** 形式を使用します。最初に、**crypto ca reference-identity** コマンドを入力して参照 ID オブジェクトを設定することで、*ca-reference-identity* モードにアクセスできます。

srv-id *value*

no srv-id *value*

構文の説明

value	各参照 ID の値。
srv-id	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。

コマンド 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	トランスペアレント	シングル	コンテキスト	システム
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

uri-non-sip

Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別するには、パラメータ コンフィギュレーション モードで **uri-non-sip** 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。

uri-non-sip action {**mask** | **log**} [**log**]

no uri-non-sip action {**mask** | **log**} [**log**]

構文の説明

ログ	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。
mask	SIP 以外の URI をマスクします。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップの Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# uri-non-sip action 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。
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。

url（crl 設定）（廃止）

CRL を取得するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードは、**クリプト CA トラストポイント** コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

構文の説明

index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。ASA は、インデックス 1 から URL を試行します。
url	CRL の取得元となる URL 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	トランスペアレント	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。**match certificate** コマンドを参照してください。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

例

次に、crl コンフィギュレーション モードを開始し、CRL 取得用の URL リストを作成およびメンテナンスするために インデックス 3 を設定し、CRL の取得元となる URL https://example.com を設定する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
ポリシー	CRL の取得元を指定します。

url（SAML IDP）

サイン インまたはサイン アウト用に SAML IdP URL を設定するには、SAML IDP コンフィギュレーション モードで **url** コマンドを使用します。SAML IDP コンフィギュレーション モードにアクセスするには、まず **webvpn** コマンドを入力します。URL を削除するには、このコマンドの **no** 形式を使用します。

url {**sign-in** | **sign-out**} **value** *url*

no url *url*

構文の説明

url	CRL の取得元となる URL 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	トランスペアレント	シングル	コンテキスト	システム
SAML IDP コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

url-block

フィルタリング サーバからのフィルタリング決定を待機する間、Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。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。

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

構文の説明

block *block_buffer*	フィルタリング サーバからのフィルタリング決定を待機している間に Web サーバの応答を保存する HTTP 応答バッファを作成します。指定できる値は 1 ～ 128 です。これは、1550 バイトのブロック数を示します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズをキロバイト（KB）単位で設定します。指定できる値は 2 ～ 10240 です。これは、2 ～ 10240 KB の URL バッファ メモリ プールを示します。
url-size *long_url_size*	バッファに保存する長い各 URL の最大許容 URL サイズを KB 単位で設定します。最大 URL サイズとして指定できる値は、Websense では 2、3、または 4（それぞれ 2 KB、3 KB、4 KB を表す）、Secure Computing では 2 または 3（それぞれ 2 KB、3 KB を表す）です。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長い URL をフィルタリングできます。Secure Computing の場合は、**url-block url-size** コマンドを使用して、最大 3 KB の長い URL をフィルタリングできます。Websense フィルタリング サーバおよび N2H2 フィルタリング サーバの場合、**url-block block** コマンドを使用すると、ASA は、URL フィルタリング サーバからの応答を待機している間、Web クライアント要求への応答として Web サーバから受信したパケットをバッファに保存します。これにより、Web クライアントのパフォーマンスがデフォルトの ASA 動作よりも向上します。デフォルトの動作では、パケットをドロップし、接続か許可された場合に Web サーバにパケットの再送信を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、ASA はブロックを HTTP 応答バッファから Web クライアントに送信し、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、ASA は拒否メッセージを Web クライアントに送信し、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答のバッファリングに使用するブロック数を指定します。

url-block url-size コマンドを **url-block mempool-size** コマンドとともに使用して、フィルタリングする URL の最大長と URL バッファに割り当てる最大メモリを指定します。Websense サーバまたは Secure-Computing サーバに、1159 バイトよりも長く、最大 4096 バイトまでの URL を渡す場合は、これらのコマンドを使用します。**url-block url-size** コマンドは、1159 バイトよりも長い URL をバッファに保存し、その URL を（TCP パケット ストリームを使用して）Websense サーバまたは Secure-Computing サーバに渡します。これにより、Websense サーバまたは Secure-Computing サーバでは、その URL へのアクセスを許可または拒否できます。

例

次に、URL フィルタリング サーバからの応答をバッファに保存するために 1550 バイトのブロックを 56 個割り当てる例を示します。

```
ciscoasa#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-cache

Websense サーバから受信した URL 応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。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。

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

構文の説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。すべてのユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有している場合に、このモードを選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求の送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、Websense サーバ上でユーザが同じ URL フィルタリング ポリシーを共有しない場合に選択します。
statistics	**statistics** オプションを使用すると、キャッシュ ルックアップの回数やヒット率などの追加の URL キャッシュ統計情報が表示されます。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

url-cache コマンドには、URL サーバからの応答をキャッシュするコンフィギュレーション オプションが用意されています。

url-cache コマンドは、URL キャッシングのイネーブル化、キャッシュ サイズの設定、およびキャッシュ統計情報の表示を行う場合に使用します。

(注) N2H2 サーバ アプリケーションは、URL フィルタリングでこのコマンドをサポートしません。

キャッシングにより、URL アクセス権限が ASA 上のメモリに保存されます。ホストが接続を要求すると、ASA は要求を Websense サーバに転送するのではなく、一致するアクセス権限を URL キャッシュ内で探します。キャッシングをディセーブルにするには、**no url-cache** コマンドを使用します。

(注) Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。目的のセキュリティ要求を満たす使用プロファイルを取得したら、**url-cache** をイネーブルにしてスループットを増大させます。Websense プロトコル バージョン 4 の URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、送信元アドレスと宛先アドレスに基づいてすべての発信 HTTP 接続をキャッシュする例を示します。

```
ciscoasa(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-server	**filter** コマンドで使用する Websense サーバを指定します。

url-entry

ポータル ページで HTTP/HTTPS URL を入力する機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **url-entry** コマンドを使用します。

url-entry enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、Finance という DAP レコードで URL 入力をイネーブルにする例を示します。

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# url-entry enable
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイ ネーブルまたはディセーブルにします。

url-length-limit

RTSP メッセージで許可される URL の最大長を設定するには、パラメータ コンフィギュレーション モードで **url-length-limit** 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。

url-length-limit *length*

no url-length-limit *length*

構文の説明

length	URL の長さ制限（バイト単位）。値の範囲は、0 ～ 6000 です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、RTSP インスペクション ポリシー マップで URL の長さ制限を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

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。

url-list

WebVPN サーバと URL のリストを特定のユーザまたはグループ ポリシーに適用するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn 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。**url-list none** コマンドを使用して作成したヌル値を含むリストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストが継承されないようにするには、**url-list none** コマンドを使用します。次回このコマンドを使用すると、前回までの設定が上書きされます。

url-list {**value** *name* | **none**} [*index*]

no url-list

構文の説明

index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み 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。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表に、このコマンドを入力す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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

次回このコマンドを使用すると、前回までの設定が上書きされます。

webvpn モードで **url-list** コマンドを使用してユーザまたはグループ ポリシーの WebVPN ホームページに表示する URL リストを指定する前に、XML オブジェクトでリストを作成する必要があります。グローバル コンフィギュレーション モードで **import** コマンドを使用して、URL リストをセキュリティ アプライアンスにダウンロードします。次に、url-list コマンドを使用して、リストを特定のグループ ポリシーまたはユーザに適用します。

例

次に、FirstGroupURLs という名前の URL リストを FirstGroup という名前のグループ ポリシーに適用し、このリストを 1 番めの URL リストに指定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

関連コマンド

コマンド	説明
clear configure url-list	すべての url-list コマンドをコンフィギュレーションから削除します。リスト名を含めると、ASA はそのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている一連の **url-list** コマンドを表示します。
webvpn	webvpn モードを開始します。これは、webvpn コンフィギュレーション モード、グループ ポリシー webvpn コンフィギュレーション モード（特定のグループ ポリシーの webvpn 設定を行う場合）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザの webvpn 設定を行う場合）のいずれかです。

url-server

filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定するには、グローバル コンフィギュレーション モードで **url-server** コマンドを使用します。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。

N2H2

url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [connections *number*]} | **UDP**]

no url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [**connections** *number*]} | **UDP**]

Websense

url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

構文の説明

N2H2

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	(任意)認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
port *number*	N2H2 サーバ ポート。ASA は、UDP 応答のリッスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、ASA は指定した次のサーバに切り替わります。デフォルトは 30 秒です。
vendor	「smartfilter」または「n2h2」(下位互換性を維持するため)を使用して URL フィルタリング サービスを指定します。ただし、「smartfilter」はベンダー文字列として保存されます。

Websense

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、ASA は指定した次のサーバに切り替わります。デフォルトは 30 秒です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル バージョン 1 です。
vendor websense	URL フィルタリング サービスのベンダーが Websense であることを示します。
version	プロトコル バージョン **1** または **4** を指定します。デフォルトは TCP プロトコル バージョン 1 です。TCP は、バージョン 1 またはバージョン 4 を使用して設定できます。UDP は、バージョン 4 を使用してのみ設定できます。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。URL サーバ数の上限は、シングル コンテキスト モードでは 16、マルチ コンテキスト モードでは 4 ですが、一度に使用できるアプリケーションは、N2H2 または Websense のいずれか 1 つのみです。さらに、ASA 上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションは更新されないため、ベンダーの指示に従って別途更新する必要があります。

HTTPS および FTP に対して **filter** コマンドを発行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連するすべての **filter** コマンドも削除されます。

サーバを指定した後、**filter url** コマンドを使用して URL フィルタリング サービスをイネーブルにします。

サーバの統計情報（到達不能サーバを含む）を表示するには、**show url-server statistics** コマンドを使用します。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1 ベンダー固有の **url-server** コマンドの適切な形式を使用して、URL フィルタリング アプリケーション サーバを指定します。

ステップ 2 **filter** コマンドを使用して、URL フィルタリングをイネーブルにします。

ステップ 3 （任意）**url-cache** コマンドを使用して、URL キャッシングをイネーブルにし、認識される応答時間を短縮します。

ステップ 4 （任意）**url-block** コマンドを使用して、長い URL および HTTP バッファリングのサポートをイネーブルにします。

ステップ 5 **show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリング サービスの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次に、N2H2 の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、Websense の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。

urgent-flag

TCP ノーマライザを通して URG ポインタを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **urgent-flag** 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。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

構文の説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタをクリアします。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトでクリアされます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈を明確化していません。したがって、エンド システムにおいては緊急オフセットがさまざまな方法で処理されます。このため、エンド システムが攻撃を受けやすくなります。デフォルトの動作では、URG フラグとオフセットはクリアされます。

例

次に、緊急フラグを許可する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 513
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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。

user

アイデンティティ ファイアウォール機能をサポートするユーザ グループ オブジェクトでユーザを作成するには、ユーザ グループ オブジェクト コンフィギュレーション モードで **user** コマンドを使用します。オブジェクトからユーザを削除するには、このコマンドの **no** 形式を使用します。

user [*domain_nickname*\]*user_name*

[no] user [*domain_nickname*\]*user_name*

構文の説明

domain_nickname	(オプション)ユーザを追加するドメインを指定します。
user_name	ユーザの名前を指定します。ユーザ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。ユーザ名にスペースを含める場合は、名前全体を引用符で囲みます。 **user** キーワードとともに指定する *user_name* 引数には ASCII ユーザ名が含まれ、IP アドレスは指定されません。

デフォルト

domain_nickname 引数を指定しない場合、ユーザはアイデンティティ ファイアウォール機能用に設定された LOCAL ドメインに作成されます。

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	トランスペアレント	シングル	コンテキスト	システム
オブジェクト グループ ユーザ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリーを送信します。これらのグループは、ASA によりアイデンティティ ファイアウォール機能用にインポートされます。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ASA は、最大 256 のユーザ グループをサポートします(インポートされたユーザ グループとローカル ユーザ グループを含む)。

アクセス グループ、キャプチャ、またはサービス ポリシー内に含めることによって、ユーザ グループ オブジェクトをアクティブにします。

ユーザ グループ オブジェクト内で、次のオブジェクト タイプを定義できます。

- **ユーザ**:オブジェクト グループ ユーザに単一のユーザを追加します。ユーザは、ローカル ユーザまたはインポートされたユーザを追加できます。

  インポートされたユーザの名前は、一意でない可能性がある一般名(cn)ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、ユーザ オブジェクトで定義したインポートされたユーザに使用できます。

- **ユーザ グループ**:Microsoft Active Directory サーバなどの外部ディレクトリ サーバによって定義されたインポートされたユーザ グループをグループ オブジェクト ユーザに追加します。

  ユーザ グループのグループ名は、一意でない可能性がある cn ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、*user-group* キーワードで指定される **user_group_name** 引数で使用できます。

  (注) *domain_nickname**user_group_name* または *domain_nickname**user_ name* を最初にオブジェクトで指定せずに、ユーザ グループ オブジェクト内に直接追加できます。*domain_nickname* が AAA サーバに関連付けられている場合、ユーザ オブジェクト グループがアクティブ化されると、ASA は詳細なネストされたユーザ グループおよび Microsoft Active Directory サーバなどの外部ディレクトリ サーバで定義されたユーザを ASA にインポートします。

- **グループ オブジェクト**:ASA でローカルに定義されたグループをオブジェクト グループ ユーザに追加します。

  (注) オブジェクト グループ ユーザ オブジェクト内にオブジェクト グループを含める場合、ACL 最適化をイネーブルにした場合にも、ASA はアクセス グループ内のオブジェクト グループを拡張しません。**show object-group** コマンドの出力には、ヒット数は表示されません。ヒット数は、ACL 最適化がイネーブルの場合に、通常のネットワーク オブジェクト グループについてのみ取得できます。

- **説明**:オブジェクト グループ ユーザの説明を追加します。

例

次に、**user** コマンドを **user-group object** コマンドとともに使用して、アイデンティティ ファイアウォール機能で使用するユーザ グループ オブジェクトにユーザを追加する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
```

```
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

関連コマンド

コマンド	説明
description	**object-group user** コマンドで作成されたグループに説明を追加します。
group-object	ローカルで定義されたオブジェクト グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたユーザ オブジェクト グループに追加します。
object-group user	アイデンティティ ファイアウォール機能用のユーザ グループ オブジェクトを作成します。
user-group	Microsoft Active Directory からインポートされたユーザ グループを **object-group user** コマンドで作成されたグループに追加します。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

user-alert

現在のアクティブ セッションのすべてのクライアントレス SSL VPN ユーザに対して、緊急メッセージのブロードキャストをイネーブルにするには、特権 EXEC モードで **user-alert** コマンドを使用します。メッセージ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。

user-alert *string cancel*

no user-alert

構文の説明

cancel	ポップアップ ブラウザ ウィンドウの起動を取り消します。
string	英数字。

デフォルト

メッセージなし。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行すると、設定されたメッセージを含むポップアップ ブラウザ ウィンドウがエンドユーザに表示されます。このコマンドでは、ASA コンフィギュレーション ファイルは変更されません。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
ciscoasa # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
ciscoasa #
```

user-authentication

ユーザ認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication 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ユーザ認証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。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。

user-authentication {**enable** | **disable**}

no user-authentication

構文の説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

個々のユーザは、設定した認証サーバの順序に従って認証されます。

プライマリ ASA でユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーのユーザ認証をイネーブルにする方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルにすると、VPN クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
secure-unit-authentication	VPN クライアントに、トンネルを開始するたびにユーザ名とパスワードによる認証を要求することによって、セキュリティを強化します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間内にユーザ接続上で通信アクティビティが行われない場合、ASA によって接続が切断されます。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。アイドル タイムアウト値が継承されないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間内にハードウェア クライアントの背後にいるユーザによって通信アクティビティが行われない場合、ASA によって接続が切断されます。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

構文の説明

minutes	アイドル タイムアウト期間の分数を指定します。指定できる範囲は 1 ～ 35791394 分です。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトまたは指定したグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されないようにします。

デフォルト

30 分。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアントのアクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前に ASA に識別情報を示すように要求します。

user-group

Microsoft Active Directory からインポートされたユーザ グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたグループに追加するには、**ユーザ グループ オブジェクト** コンフィギュレーション モードで **user-group** コマンドを使用します。オブジェクトからユーザ グループを削除するには、このコマンドの **no** 形式を使用します。

user-group [*domain_nickname*\]*user_group_name*

[no] user-group [*domain_nickname*\]*user_group_name*

構文の説明

domain_nickname	(オプション)ユーザ グループを作成するドメインを指定します。
user_group_name	ユーザ グループの名前を指定します。グループ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。グループ名にスペースを含める場合は、名前全体を引用符で囲みます。

デフォルト

domain_nickname 引数を指定しない場合、ユーザ グループはアイデンティティ ファイアウォール機能用に設定された LOCAL ドメインに作成されます。

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	トランスペアレント	シングル	コンテキスト	システム
オブジェクト グループ ユーザ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリーを送信します。これらのグループは、ASA によりアイデンティティ ファイアウォール機能用にインポートされます。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ASA は、最大 256 のユーザ グループをサポートします(インポートされたユーザ グループとローカル ユーザ グループを含む)。

アクセス グループ、キャプチャ、またはサービス ポリシー内に含めることによって、ユーザ グループ オブジェクトをアクティブにします。

ユーザ グループ オブジェクト内で、次のオブジェクト タイプを定義できます。

- **ユーザ**:オブジェクト グループ ユーザに単一のユーザを追加します。ユーザは、ローカル ユーザまたはインポートされたユーザを追加できます。

  インポートされたユーザの名前は、一意でない可能性がある一般名(cn)ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、ユーザ オブジェクトで定義したインポートされたユーザに使用できます。

- **ユーザ グループ**:Microsoft Active Directory サーバなどの外部ディレクトリ サーバによって定義されたインポートされたユーザ グループをグループ オブジェクト ユーザに追加します。

  ユーザ グループのグループ名は、一意でない可能性がある cn ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、*user-group* キーワードで指定される **user_group_name** 引数で使用できます。

  (注) *domain_nickname**user_group_name* または *domain_nickname**user_ name* を最初にオブジェクトで指定せずに、ユーザ グループ オブジェクト内に直接追加できます。*domain_nickname* が AAA サーバに関連付けられている場合、ユーザ オブジェクト グループがアクティブ化されると、ASA は詳細なネストされたユーザ グループおよび Microsoft Active Directory サーバなどの外部ディレクトリ サーバで定義されたユーザを ASA にインポートします。

- **グループ オブジェクト**:ASA でローカルに定義されたグループをオブジェクト グループ ユーザに追加します。

  (注) オブジェクト グループ ユーザ オブジェクト内にオブジェクト グループを含める場合、ACL 最適化をイネーブルにした場合にも、ASA はアクセス グループ内のオブジェクト グループを拡張しません。**show object-group** コマンドの出力には、ヒット数は表示されません。ヒット数は、ACL 最適化がイネーブルの場合に、通常のネットワーク オブジェクト グループについてのみ取得できます。

- **説明**:オブジェクト グループ ユーザの説明を追加します。

例

次に、**user-group** コマンドを **user-group object** コマンドとともに使用して、アイデンティティ ファイアウォール機能で使用するユーザ グループ オブジェクトにユーザ グループを追加する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
```

```
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

関連コマンド

コマンド	説明
description	**object-group user** コマンドで作成されたグループに説明を追加します。
group-object	ローカルで定義されたオブジェクト グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたユーザ オブジェクト グループに追加します。
object-group user	アイデンティティ ファイアウォール機能用のユーザ グループ オブジェクトを作成します。
user	**object-group user** コマンドで作成されたオブジェクト グループにユーザを追加します。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

user-identity action ad-agent-down

Active Directory エージェントが応答不能の場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action ad-agent-down** コマンドを使用します。アイデンティティ ファイアウォール インスタンスに対するこのアクションを削除するには、このコマンドの **no** 形式を使用します。

user-identity action ad-agent-down disable-user-identity-rule

no user-identity action ad-agent-down disable-user-identity-rule

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

デフォルトでは、このコマンド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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

AD エージェントが応答していない場合のアクションを指定します。

AD エージェントがダウンし、**user-identity action ad-agent-down** コマンドが設定されている場合、ASA はそのドメインのユーザに関連付けられたユーザ アイデンティティ ルールをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action domain-controller-down

Active Directory ドメイン コントローラが応答不能の場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action domain-controller-down** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

no user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

構文の説明

domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。

デフォルト

デフォルトでは、このコマンド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。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

Active Directory ドメイン コントローラが応答しないためにドメインがダウンしている場合のアクションを指定します。

ドメインがダウンし、**disable-user-identity-rule** キーワードが設定されている場合、ASA はそのドメインのユーザ アイデンティティと IP アドレスのマッピングをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションを設定する例を示します。

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action mac-address-mismatch

ユーザの MAC アドレスが ASA デバイス IP アドレスと一致しないことが明らかになった場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action mac-address mismatch** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action mac-address mismatch remove-user-ip

no user-identity action mac-address mismatch remove-user-ip

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

デフォルトでは、このコマンドが指定されている場合、ASA は **remove-user-ip** を使用します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザの MAC アドレスが、そのアドレスに現在マッピングされている ASA デバイス IP アドレスと一致しないことが明らかになった場合のアクションを指定します。このアクションは、ユーザ アイデンティティ ルールの効果を無効にします。

user-identity action mac-address-mismatch コマンドが設定されている場合、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action netbios-response-fail

クライアントが NetBIOS プローブに応答しない場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action netbios-response-fail** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action netbios-response-fail remove-user-ip

no user-identity action netbios-response-fail remove-user-ip

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

デフォルトでは、このコマンド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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

クライアントが NetBIOS プローブに応答しない場合のアクションを指定します。このような状況には、そのクライアントへのネットワーク接続がブロックされている場合やクライアントがアクティブでない場合などがあります。

user-identity action remove-user-ip コマンドを設定すると、ASA は、そのクライアントのユーザアイデンティティと IP アドレスのマッピングを削除します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent aaa-server

Cisco Identity Firewall インスタンスの AD エージェントのサーバ グループを定義するには、AAA サーバ ホスト コンフィギュレーション モードで **user-identity ad-agent aaa-server** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

no user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

構文の説明

aaa_server_group_tag	アイデンティティ ファイアウォールに関連付けられた AAA サーバ グループを指定します。

デフォルト

このコマンドには、デフォルトはありません。

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

aaa_server_group_tag 変数に定義する最初のサーバがプライマリ AD エージェントとなり、次に定義するサーバがセカンダリ AD エージェントとなります。

アイデンティティ ファイアウォールでは、2 つの AD エージェント ホストのみ定義できます。

プライマリ AD エージェントがダウンしていることを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの AAA サーバは通信プロトコルとして RADIUS を使用するため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールの AD エージェントの AAA サーバ ホストを定義する例を示します。

```
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent active-user-database

ASA が Cisco Identity Firewall インスタンスの AD エージェントからユーザ アイデンティティと IP アドレスのマッピング情報を取得する方法を定義するには、グローバル コンフィギュレーション モードで **user-identity ad-agent active-user-database** コマンドを使用します。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。

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

no user-identity ad-agent active-user-database {**on-demand** | **full-download**}

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

デフォルトでは、ASA 5505 は on-demand オプションを使用します。それ以外の ASA プラットフォームは full-download オプションを使用します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が AD エージェントからユーザ アイデンティティと IP アドレスのマッピング情報を取得する方法を定義します。

- **full-download**：ASA が、ASA の起動時に IP/ユーザ マッピング テーブル全体をダウンロードし、ユーザのログインおよびログアウト時に増分 IP/ユーザ マッピングを受信するように指示する要求を AD エージェントに送信することを指定します。
- **on-demand**：ASA が新しい接続を必要とするパケットを受信し、その送信元 IP アドレスのユーザがユーザ アイデンティティ データベースに含まれていない場合に、ASA が AD エージェントから IP アドレスのユーザ マッピング情報を取得することを指定します。

デフォルトでは、ASA 5505 は on-demand オプションを使用します。それ以外の ASA プラットフォームは full-download オプションを使用します。

フル ダウンロードはイベント ドリブンです。つまり、2 回目以降のデータベース ダウンロード要求は、ユーザ アイデンティティと IP アドレス マッピング データベースの更新内容だけを送信します。

ASA が変更要求を AD エージェントに登録すると、AD エージェントは新しいイベントを ASA に送信します。

例

次に、アイデンティティ ファイアウォールに対してこのオプションを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent hello-timer

ASA と Cisco Identity Firewall インスタンスの AD エージェントとの間のタイマーを定義するには、グローバル コンフィギュレーション モードで **user-identity ad-agent hello-timer** コマンドを使用します。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。

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

no user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

構文の説明

number	タイマーのリトライ回数を指定します。
seconds	タイマーの時間の長さを指定します。

デフォルト

デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA と AD エージェントとの間の Hello タイマーを定義します。

ASA と AD エージェントとの間の Hello タイマーは、ASA が hello パケットを交換する頻度を定義します。ASA は、hello パケットを使用して、ASA 複製ステータス（in-sync または out-of-sync）とドメイン ステータス（up または down）を取得します。ASA は、AD エージェントから応答を受信しなかった場合、指定された間隔が経過した後、hello パケットを再送信します。

デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

例

次に、アイデンティティ ファイアウォールに対してこのオプションを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent event-timestamp-check

認可変更リプレイ アタックから ASA を保護するために RADIUS イベント タイムスタンプ チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **user-identity ad-agent event-timestamp-check** コマンドを使用します。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。

user-identity ad-agent event-timestamp-check

no user-identity ad-agent event-timestamp-check

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

デフォルト設定で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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ASA が受信する各 ID の最後のイベントのタイムスタンプを追跡し、イベントのタイムスタンプが ASA のクロックより 5 分以上古い場合、またはメッセージのタイムスタンプが最後のイベントのタイムスタンプよりも前の場合にメッセージを廃棄することを可能にします。

最後のイベントのタイムスタンプの情報を持たない新しく起動した ASA の場合、ASA は自身のクロックとイベントのタイムスタンプを比較します。イベントから少なくとも 5 分以上経過している場合、ASA はメッセージを受け入れません。

（注） NTP を使用して、ASA、Active Directory、および Active Directory エージェントをそれらのクロックが相互に同期するように設定することを推奨します。

例

次に、アイデンティティ ファイアウォールにイベント タイムスタンプ チェックを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

関連コマンド

コマンド	説明
user-identity ad-agent hello-timer	ASA と Cisco Identity Firewall インスタンスの AD エージェントとの間のタイマーを定義します。

user-identity default-domain

Cisco Identity Firewall インスタンスのデフォルト ドメインを指定するには、グローバル コンフィギュレーション モードで **user-identity default-domain** コマンドを使用します。デフォルト ドメインを削除するには、このコマンドの **no** 形式を使用します。

user-identity default-domain *domain_NetBIOS_name*

no user-identity default-domain *domain_NetBIOS_name*

構文の説明

domain_NetBIOS_name	アイデンティティ ファイアウォールのデフォルト ドメインを指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	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_NetBIOS_name には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に「.」と「 」(スペース) を使用することはできません。ドメイン名にスペースを含める場合は、名前全体を引用符で囲みます。ドメイン名では、大文字と小文字が区別されません。

デフォルト ドメインは、ユーザまたはグループにドメインが明示的に設定されていない場合に、すべてのユーザおよびユーザ グループで使用されます。デフォルト ドメインを指定しない場合、ユーザおよびグループのデフォルト ドメインは LOCAL となります。マルチ コンテキスト モードでは、システム実行スペース内だけでなく、各コンテキストについてデフォルト ドメイン名を設定できます。

(注) 指定するデフォルト ドメイン名は、Active Directory ドメイン コントローラに設定された NetBIOS ドメイン名と一致している必要があります。ドメイン名が一致しない場合、AD エージェントは、ユーザ アイデンティティと IP アドレスのマッピングを ASA の設定時に入力されたドメイン名に誤って関連付けます。NetBIOS ドメイン名を表示するには、任意のテキスト エディタで Active Directory ユーザ イベント セキュリティ ログを開きます。

アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザに対して LOCAL ドメインを使用します。Web ポータル（カットスルー プロキシ）経由でログインしたユーザは、認証された Active Directory ドメインに属すると見なされます。VPN 経由でログインしたユーザは、VPN が Active Directory で LDAP によって認証される場合を除き、LOCAL ドメインに属するユーザと見なされます。これにより、アイデンティティ ファイアウォールはユーザをそれぞれの Active Directory ドメインに関連付けることができます。

例

次に、アイデンティティ ファイアウォールのデフォルト ドメインを設定する例を示します。

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity domain

Cisco Identity Firewall インスタンスのドメインを関連付けるには、グローバル コンフィギュレーション モードで **user-identity domain** コマンドを使用します。ドメインの関連付けを削除するには、このコマンドの **no** 形式を使用します。

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

no user-identity *domain_nickname* **aaa-server** *aaa_server_group_tag*

構文の説明

aaa_server_group_tag	アイデンティティ ファイアウォールに関連付けられた AAA サーバ グループを指定します。
domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

AAA サーバでユーザ グループ クエリーのインポート用に定義された LDAP パラメータをドメイン名に関連付けます。

domain_nickname には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に「.」と「 」(スペース)を使用することはできません。ドメイン名にスペースを含める場合は、スペースを引用符で囲む必要があります。ドメイン名では、大文字と小文字が区別されません。

例

次に、アイデンティティ ファイアウォールのドメインを関連付ける例を示します。

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity enable

Cisco Identity Firewall インスタンスを作成するには、グローバル コンフィギュレーション モードで **user-identity enable** コマンドを使用します。アイデンティティ ファイアウォール インスタン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。

user-identity enable

no user-identity enable

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、アイデンティティ ファイアウォールをイネーブルにします。

例

次に、アイデンティティ ファイアウォールをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity enable
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity inactive-user-timer

Cisco Identity Firewall インスタンスでユーザがアイドル状態であると見なされるまでの時間を指定するには、グローバル コンフィギュレーション モードで **user-identity inactive-user-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

user-identity inactive-user-timer minutes *minutes*

no user-identity inactive-user-timer minutes *minutes*

構文の説明

minutes	ユーザがアイドル状態であると見なされるまでの時間を分単位で指定します。これは、ASA が指定された時間にわたりユーザの IP アドレスからトラフィックを受信しなかった場合を意味します。

デフォルト

デフォルトでは、アイドル タイムアウトは 60 分に設定されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

タイマーの期限が切れると、ユーザの IP アドレスが非アクティブとマークされ、ローカル キャッシュ内のユーザ アイデンティティと IP アドレスのマッピング データベースから削除されます。ASA は、この IP アドレスの削除を AD エージェントに通知しません。既存のトラフィックは通過を許可されます。このコマンドを指定すると、ASA は NetBIOS ログアウト プローブが設定されている場合でも非アクティブ タイマーを実行します。

(注) アイドル タイムアウト オプションは VPN ユーザまたはカットスルー プロキシ ユーザには適用されません。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity logout-probe

Cisco Identity Firewall インスタンスに対する NetBIOS プローブをイネーブルにするには、グローバル コンフィギュレーション モードで **user-identity logout-probe** コマンドを使用します。プローブを削除して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。

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

no user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

構文の説明

minutes	プローブ間隔を分単位で指定します。
seconds	リトライ インターバルの時間の長さを指定します。
times	プローブのリトライ回数は、次のように指定してください。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

NetBIOS パケットを最小限に抑えるために、ASA は、ユーザが指定された分数を超えてアイドル状態である場合のみ NetBIOS プローブをクライアントに送信します。

NetBIOS プローブ タイマーを 1 ～ 65535 分に設定し、リトライ インターバルを 1 ～ 256 回に設定します。プローブのリトライ回数は、次のように指定してください。

- **match-any**：クライアントからの NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名が含まれている場合、ユーザ アイデンティティは有効と見なされます。このオプションを指定するためには、クライアントで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。

- **exact-match**：NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名だけが含まれている必要があります。そうでない場合、その IP アドレスのユーザ アイデンティティは無効と見なされます。このオプションを指定するためには、クライアントで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。
- **user-not-needed**：ASA がクライアントから NetBIOS 応答を受信した場合、ユーザ アイデンティティは有効と見なされます。

アイデンティティ ファイアウォールは、少なくとも 1 つのセキュリティ ポリシーに存在するアクティブ状態のユーザ アイデンティティに対してのみ NetBIOS プローブを実行します。ASA は、ユーザがカットスルー プロキシ経由または VPN を使用してログインするクライアントについては、NetBIOS プローブを実行しません。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity monitor

クラウド Web セキュリティのために、指定されたユーザまたはグループの情報を AD エージェントからダウンロードするには、グローバル コンフィギュレーション モードで user-identity monitor コマンドを使用します。モニタリングを停止にするには、このコマンドの **no** 形式を使用します。

user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

no user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

構文の説明

object-group-user *object-group-name*	オブジェクト グループ ユーザ名を指定します。このグループには、複数のグループを含めることができます。
user-group [*domain-name*\\] *group-name*	グループ名をインラインで指定します。ドメインとグループの間に 2 つのバックスラッシュ (\\) を指定しますが、ASA は、クラウド Web セキュリティへの送信時に、クラウド Web セキュリティの表記規則に準拠するようにバックスラッシュが 1 つのみ含まれるように名前を変更します。

コマンド 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォール機能を使用する場合、ASA は、アクティブな ACL に含まれるユーザおよびグループの AD サーバからのユーザ アイデンティティ情報のみをダウンロードします。ACL は、アクセス ルール、AAA ルール、サービス ポリシー ルール、またはアクティブと見なされるその他の機能で使用する必要があります。クラウド Web セキュリティでは、そのポリシーがユーザ アイデンティティに基づくことができるため、すべてのユーザに対する完全なアイデンティティ ファイアウォール カバレッジを取得するには、アクティブな ACL の一部ではないグループをダウンロードする必要があります。たとえば、ユーザおよびグループを含む ACL を使用するようにクラウド Web セキュリティ サービス ポリシー ルールを設定し、関連するグループをアクティブ化できますが、これは必須ではありません。IP アドレスのみに基づく ACL を使用できます。ユーザ アイデンティティ モニタ機能では、AD エージェントからグループ情報を直接ダウンロードすることができます。

ASA は、ユーザ アイデンティティ モニタ用に設定されたグループ、アクティブな ACL によってモニタされているグループも含めて 512 以下のグループモニタできます。

例

次に、CISCO\\Engineering ユーザ グループをモニタする例を示します。

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。

コマンド	説明
show scansafe statistics	合計と現在の HTTP 接続を表示します。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

user-identity poll-import-user-group-timer

ASA が Active Directory サーバに Cisco Identity Firewall インスタンスのユーザ グループ情報を問い合わせるまでの時間を指定するには、グローバル コンフィギュレーション モードで **user-identity poll-import-user-group-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

user-identity poll-import-user-group-timer hours *hours*

no user-identity poll-import-user-group-timer hours *hours*

構文の説明

hours	poll タイマーの時間を設定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が Active Directory サーバにユーザ グループ情報を問い合わせるまでの時間を指定します。

Active Directory グループでユーザが追加または削除されると、ASA はグループ インポート タイマーの実行後に更新されたユーザ グループを受け取ります。

デフォルトでは、poll タイマーは 8 時間です。

ユーザ グループ情報をただちに更新するには、**user-identity update import-user** コマンドを入力します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity static user

新しいユーザと IP アドレスのマッピングを作成するか、Cisco Identity Firewall 機能でユーザの IP アドレスを非アクティブに設定するには、グローバル コンフィギュレーション モードで **user-identity static user** コマンドを使用します。アイデンティティ ファイアウォールでこの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。

user-identity static user [*domain*\] *user_name host_ip*

no user-identity static user [*domain*\] *user_name host_ip*

構文の説明

domain	新しいユーザと IP アドレスのマッピングを作成するか、指定したドメインのユーザの IP アドレスを非アクティブに設定します。
host_ip	新しいユーザと IP アドレスのマッピングを作成するか、非アクティブに設定するユーザの IP アドレスを指定します。
user_name	新しいユーザと IP アドレスのマッピングを作成するか、IP アドレスを非アクティブに設定するユーザのユーザ名を指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインはありません。

例

次に、user1 の静的マッピングを作成する例を示します。

```
ciscoasa(config)# user-identity static user SAMPLE\user1 192.168.1.101
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity update active-user-database

Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードするには、グローバル コンフィギュレーション モードで **user-identity update active-user-database** コマンドを使用します。

user-identity update active-user-database [**timeout minutes** *minutes*]

構文の説明

minutes	タイムアウトの分数を指定します。

デフォルト

デフォルトのタイムアウトは 5 分です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードします。

このコマンドは、更新処理を開始し、更新開始ログを生成して即座に返します。更新処理が終了するか、タイマーの期限切れで中断すると、別の syslog メッセージが生成されます。1 つの未処理の更新処理だけが許可されます。コマンドを再実行すると、エラー メッセージが表示されます。

コマンドの実行が終了すると、ASA によってコマンド プロンプトに [Done] が表示され、syslog メッセージが生成されます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa# user-identity update active-user-database
ERROR: one update active-user-database operation is already in progress
[Done] user-identity update active-user-database
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity update import-user

Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードするには、グローバル コンフィギュレーション モードで **user-identity update active-user-database** コマンドを使用します。

user-identity update import-user [[*domain_nickname*\\] *user_group_name* [**timeout seconds** *seconds*]]

構文の説明

domain_nickname	更新するグループのドメインを指定します。
seconds	タイムアウトの秒数を指定します。
user_group_name	*user_group_name* を指定した場合、指定したインポート ユーザ グループだけが更新されます。アクティブ化されたグループのみ(たとえば、アクセス グループ、アクセス リスト、キャプチャ、サービス ポリシー内のグループ)を更新することができます。 指定したグループがアクティブ化されていない場合、このコマンドは処理を拒否します。指定したグループに複数の階層レベルがある場合は、再帰 LDAP クエリーが実行されます。 *user_group_name* を指定しない場合、ASA は LDAP 更新サービスを即座に開始し、すべてのアクティブ化されたグループの更新を定期的に試行します。

デフォルト

ASA は更新を最大 5 回再試行し、必要に応じて警告メッセージを生成します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ポーリング インポート ユーザ グループ タイマーの満了を待たずに即時に Active Directory サーバを照会して、指定されたインポート ユーザ グループ データベースを更新します。ローカル ユーザ グループで設定が変更されるたびにグループ ID データベースが更新されるため、ローカル ユーザ グループを更新するコマンドはありません。

このコマンドは、コンソールが LDAP クエリーの戻りを待機することを妨げません。

このコマンドは、更新処理を開始し、更新開始ログを生成して即座に返します。更新処理が終了するか、タイマーの期限切れで中断すると、別の syslog メッセージが生成されます。1 つの未処理の更新処理だけが許可されます。コマンドを再実行すると、エラー メッセージが表示されます。

LDAP クエリーが成功した場合、ASA は取得したユーザ データをローカル データベースに保存し、ユーザ/グループの関連付けを必要に応じて変更します。更新処理が成功した場合、**show user-identity user-of-group** *domain**group* コマンドを実行して、このグループの下に保存されたすべてのユーザを一覧表示できます。

ASA は、各アップデート後に、インポートされたすべてのグループをチェックします。アクティブ化された Active Directory グループが Active Directory に存在しない場合、ASA は syslog メッセージを生成します。

user_group_name を指定しない場合、ASA は LDAP 更新サービスを即座に開始し、すべてのアクティブ化されたグループの更新を定期的に試行します。LDAP 更新サービスはバックグラウンドで実行され、Active Directory サーバで LDAP クエリーによってインポート ユーザ グループを定期的に更新します。

システムのブートアップ時に、アクセス グループで定義されたインポート ユーザ グループがある場合、ASA は LDAP クエリーによってユーザ/グループ データを取得します。更新中にエラーが発生した場合、ASA は更新を最大 5 回再試行し、必要に応じて警告メッセージを生成します。

コマンドの実行が終了すると、ASA によってコマンド プロンプトに [Done] が表示され、syslog メッセージが生成されます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa# user-identity update import-user group.sample-group1
ERROR: Update import-user group is already in progress
[Done] user-identity update import-user group.sample-group1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity user-not-found

Cisco Identity Firewall インスタンスの user-not-found 追跡をイネーブルにするには、グローバル コンフィギュレーション モードで **user-identity user-not-found** コマンドを使用します。アイデンティティ ファイアウォール インスタンスでこの追跡を削除するには、このコマンドの **no** 形式を使用します。

user-identity user-not-found enable

no user-identity user-not-found enable

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

デフォルトでは、このコマンド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。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

最後の 1024 個の IP アドレスだけがトラッキングされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity user-not-found enable
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-message

DAP レコードが選択されたときに表示するテキスト メッセージを指定するには、ダイナミック アクセス ポリシー レコード モードで user-message コマンドを使用します。このメッセージを削除するには、このコマンドの **no** 形式を使用します。同じ DAP レコードに対してコマンドを複数回使用した場合、前のメッセージは新しいメッセージに置き換えられます。

user-message *message*

no user-message

構文の説明

message	この DAP レコードに割り当てられているユーザに対するメッセージ。最大 128 文字を入力できます。メッセージにスペースを含める場合は、メッセージを二重引用符で囲みます。

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	トランスペアレント	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

SSL VPN 接続に成功すると、ポータル ページに、クリック可能な点滅するアイコンが表示されます。ユーザはそのアイコンをクリックして、接続に関連付けられているメッセージを確認できます。DAP ポリシーからの接続が終了し（アクション = 終了）、その DAP レコードにユーザ メッセージが設定されている場合は、そのメッセージがログイン画面に表示されます。

複数の DAP レコードが接続に適用される場合、ASA は該当するユーザ メッセージを組み合わせて 1 つのストリングとして表示します。

例

次に、Finance という DAP レコードに「Hello Money Managers」というユーザ メッセージを設定する例を示します。

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# user-message "Hello Money Managers"
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

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

user-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **user-parameter** を使用します。

user-parameter *name*

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

構文の説明

string	HTTP POST 要求に含まれているユーザ名パラメータの名前。名前の最大の長さは 128 文字です。

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

これは HTTP フォームのコマンドを使用した SSO です。ASA の WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。要求されたコマンド **user-parameter** は、HTTP POST 要求に SSO 認証用のユーザ名パラメータを含める必要があることを指定します。

(注) ログイン時に、ユーザは実際の名前を入力します。この名前は、HTTP POST 要求に入力されて認証 Web サーバに渡されます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、SSO 認証に使用される HTTP POST 要求にユーザ名パラメータ userid を含めることを指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。

user-statistics

MPF によるユーザ統計情報の収集をアクティブ化し、アイデンティティ ファイアウォールの検索アクションを一致させるには、ポリシー マップ コンフィギュレーション モードで **user-statistics** コマンドを使用します。ユーザ統計情報の収集を削除するには、このコマンドの **no** 形式を使用します。

user-statistics [**accounting** | **scanning**]

no user-statistics [**accounting** | **scanning**]

構文の説明

accounting	（オプション）ASA が送信パケット数、送信ドロップ数、および受信パケット数を収集することを指定します。
scanning	（オプション）ASA が送信ドロップ数のみを収集することを指定します。

デフォルト

デフォルトでは、このコマンド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	トランスペアレント	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザ統計情報を収集するようポリシー マップを設定すると、ASA は選択したユーザの詳細な統計情報を収集します。**accounting** または **scanning** キーワードを指定せずに **user-statistics** コマンドを指定した場合、ASA はアカウンティング統計情報とスキャンの統計情報の両方を収集します。

例

次に、アイデンティティ ファイアウォールに対してユーザ統計情報をアクティブ化する例を示します。

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map p-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
ciscoasa(config-pmap)# user-statistics accounting
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy p-identity-example-1 interface outside
```

関連コマンド

コマンド	説明
policy-map	モジュラ ポリシー フレームワークの使用時に、レイヤ 3/4 クラスマップで特定したトラフィックにアクションを割り当てます。
service-policy（グローバル）	すべてのインターフェイスまたは対象のインターフェイスでポリシー マップをグローバルにアクティブ化します。
show service-policy [**user-statistics**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、設定されたサービス ポリシーのユーザ統計情報を表示します。
show user-identity ip-of-user [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、指定したユーザの IP アドレスについて受信パケット、送信パケット、およびドロップ統計情報を表示します。
show user-identity user active [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、アクティブ ユーザについて指定期間の受信パケット、送信パケット、およびドロップ統計情報を表示します。
show user-identity user-of-ip [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、指定した IP アドレスのユーザの受信パケット、送信パケット、およびドロップ統計情報を表示します。
user-identity enable	アイデンティティ ファイアウォール インスタンスを作成します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn コンフィギュレーション モードで **user storage** コマンドを使用します。ユーザ ストレージ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。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。 ユーザ名とパスワードが NETFS-location に組み込まれている場合、パスワード入力はクリアとして扱われます。

デフォルト

ユーザストレージ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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.4(6)	**show run** の実行時にパスワードがクリア テキストで表示されないようになりました。

使用上のガイドライン

ユーザ ストレージを使用すると、キャッシュされた資格情報およびクッキーを、ASA フラッシュ以外の場所に保存できます。このコマンドは、クライアントレス SSL VPN ユーザの個人用ブックマークにシングル サイン オンを提供します。ユーザ資格情報は、複合できない <user_id>.cps ファイルとして FTP/CIFS/SMB サーバに暗号化形式で保存されます。

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、ASA ではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

データが外部の FTP サーバまたは SMB サーバで暗号化されている場合は、ブックマークの追加を選択してポータル ページ内に個人用ブックマークを定義できます（例：user-storage cifs://jdoe:test@10.130.60.49/SharedDocs）。すべてのプラグイン プロトコルにも個人用 URL を作成できます。

（注） すべてが同じ FTP/CIFS/SMB サーバを参照して同じ「ストレージ キー」を使用する ASA のクラスタがある場合は、クラスタ内のどの ASA を介してもブックマークにアクセスできます。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
ciscoasa(config)# wgroup-policy DFLTGrpPolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
ciscoasa(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	セッション間で保管されたデータを保護するためのストレージ キーを指定します。
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

username

ユーザを ASA ローカル データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名を指定して、このコマンドの **no** 形式を使用します。

username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

no username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

構文の説明

encrypted	9.6 以前の場合は、32 文字以内のパスワードは暗号化されることを示します（**mschap** を指定しなかった場合）。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するとき MD5 ハッシュを作成します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 9.7 以降では、すべての長さのパスワードで PBKDF2 を使用します。
mschap	パスワードを入力後に Unicode に変換し、MD4 を使用してハッシュすることを指定します。このキーワードは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
name	3 ～ 64 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字を使用して、ユーザ名を指定します。
nopassword	このユーザの*任意の*パスワードを入力できることを示します。これは安全な設定ではないため、このキーワードの使用には注意してください。 (9.6(2) 以降）パスワードなしでユーザ名を作成するには、**password** または **nopassword** キーワードを入力しないでください。たとえば、**ssh authentication** コマンドを使用すると、ASA に公開キーをインストールして、SSH クライアントでプライベート キーを使用できます。そのため、パスワード設定が不要な場合があります。

nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 で使用するために暗号化することを示します。ユーザを追加するときに **mschap** キーワードを指定した場合は、**show running-config** コマンドを使用してコンフィギュレーションを表示すると、**encrypted** キーワードではなくこのキーワードが表示されます。 **username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **nt-encrypted** キーワードが示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` CLI で実際に **nt-encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストし、かつ、同じパスワードを使用する場合のみです。
password *password*	3 ～ 32 文字（9.5 以前）または 127 文字（9.6 以降）の、スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）でパスワードを設定します。
pbkdf2	パスワードの暗号化を指定します。9.6 以前の場合、PBKDF2（パスワードベースのキー派生関数 2）ハッシュは、パスワードの長さが 32 文字を超える場合にのみ使用されます。9.7 以降では、すべてのパスワードで PBKDF2 を使用します。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに PBKDF2 ハッシュを作成します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **pbkdf2** キーワードが示されます。たとえば、長いパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s pbkdf2` CLI で実際に **pbkdf2** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意してください。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）の範囲で設定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンド認可で使用されます。

デフォルト　デフォルトの特権レベルは 2 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。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが追加されました。
7.2(1)	**mschap** キーワードと **nt-encrypted** キーワードが追加されました。
9.6(1)	パスワードの長さが 127 文字に増加し、**pbkdf2** キーワードが追加されました。
9.6(2)	**password** または **nopassword** キーワードを使用せずにユーザ名を作成できるようになりました。
9.7(1)	すべての長さのパスワードが PBKDF2 ハッシュを使用してコンフィギュレーションに保存されるようになりました。

使用上のガイドライン

login コマンドでは、このデータベースを認証用に使用します。

CLI にアクセスできるユーザや特権モードを開始できないユーザをローカル データベースに追加する場合は、コマンド認可をイネーブルにする必要があります（**aaa authorization command** コマンドを参照してください）。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、AAA 認証を使用してユーザが **login** コマンドを使用できないようにするか、すべてのローカル ユーザをレベル 1 に設定して **enable** パスワードで特権 EXEC モードにアクセスできるユーザを制御できます。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。

パスワード認証ポリシーがイネーブルの場合、**username** コマンドを使用して自身のパスワードを変更したり、自身のアカウントを削除したりできません。ただし、パスワードは **change-password** コマンドを使用して変更できます。

ユーザ名パスワード日付を表示するには、**show running-config all username** コマンドを使用します。

例

次に、パスワードが 12345678、特権レベルが 12 の「anyuser」という名前のユーザを設定する例を示します。

```
ciscoasa(config)# username anyuser password 12345678 privilege 12
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username attributes

ユーザ名属性モードを開始するには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザの属性をすべて削除するには、このコマンドの **no** 形式を使用し、ユーザ名を付加します。すべてのユーザの属性をすべて削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。属性モードを使用すると、指定したユーザに対して属性値ペアを設定できます。

username *name* **attributes**

no username *name* **attributes**

構文の説明

name	ユーザ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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	**service-type** 属性が追加されました。
9.1(2)	**ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} 属性が追加されました。

使用上のガイドライン

内部ユーザ認証データベースは、**username** コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザ名属性は、**username** コマンドまたは **username attributes** コマンドを使用して設定できます。

ユーザ名コンフィギュレーション モードのコマンド構文には、一般に次の特性があります。

- **no** 形式を使用すると、実行コンフィギュレーションから属性が削除されます。
- **none** キーワードを使用しても、実行コンフィギュレーションから属性が削除されます。ただし、このキーワードでは、属性をヌル値に設定し、継承されないようにすることによって、このことを行います。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

username attributes コマンドは、ユーザ名属性モードを開始し、次の属性を設定できるようにします。

属性	機能
group-lock	ユーザが接続する必要がある既存のトンネル グループを指定します。
password-storage	クライアント システムでのログイン パスワードの保存をイネーブルまたはディセーブルにします。
service-type [**remote-access** | **admin** | **nas-prompt**]	コンソール ログインを制限し、適切なレベルが割り当てられているユーザのログインをイネーブルにします。**remote-access** オプションでは、リモート アクセスのための基本的な AAA サービスを指定します。**admin** オプションは、AAA サービス、ログイン コンソール特権、EXEC モード特権、イネーブル特権、および CLI 特権を指定します。**nas-prompt** オプションは、AAA サービス、ログイン コンソール特権、および EXEC モード特権を指定しますが、イネーブル特権は指定しません。

属性	機能
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	公開キー認証をユーザ単位でイネーブルにします。*key* 引数の値は次のいずれかになります。 • *key* 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、SSH-RSA の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります(つまり、証明書は使用しません)。Base 64 エンコード公開キーを送信すると、そのキーは SHA-256 によりハッシュ化され、それ以降のすべての比較では対応する 32 バイト ハッシュが使用されます。 • *key* 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります(解析のため)。 **pkf** オプションを使用すると、4096 ビットの RSA キーを SSH 公開キー ファイル(PKF)として使用して認証を行うことができます。このオプションは、4096 ビットの RSA キーに制限されず、4096 ビット RSA キー未満の任意のサイズに使用できます。 **nointeractive** オプションは、SSH 公開キー形式のキーをインポートするときにすべてのプロンプトを抑制します。この非インタラクティブ データ入力モードは ASDM での使用のみを目的としています。 *key* フィールドおよび **hashed** キーワードは **publickey** オプションでのみ使用でき、**nointeractive** キーワードは **pkf** オプションでのみ使用できます。 設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA のリブート時に使用されます。 (注) PKF オプションはフェールオーバーがイネーブルの場合に使用できますが、PKF データはスタンバイ システムに自動的に複製されません。**write standby** コマンドを入力して、フェールオーバー ペアのスタンバイ システムに PKF 設定を同期する必要があります。
vpn-access-hours	設定済みの時間範囲ポリシーの名前を指定します。
vpn-filter	ユーザ固有の ACL の名前を指定します。
vpn-framed-ip-address	クライアントに割り当てる IP アドレスとネットマスクを指定します。
vpn-group-policy	属性の継承元となるグループ ポリシーの名前を指定します。
vpn-idle-timeout [**alert-interval**]	アイドルタイムアウト期間を分単位で指定するか、または **none** を指定してディセーブルにします。任意で、タイムアウト前のアラート間隔を指定します。
vpn-session-timeout [**alert-interval**]	最大ユーザ接続時間を分単位で指定するか、または **none** を指定して時間を無制限にします。任意で、タイムアウト前のアラート間隔を指定します。

属性	機能
vpn-simultaneous-logins	許可される同時ログインの最大数を指定します。
vpn-tunnel-protocol	使用できるトンネリング プロトコルを指定します。
webvpn	ユーザ名 webvpn コンフィギュレーション モードを開始し、WebVPN 属性を設定できるようにします。

ユーザ名の webvpn モード属性を設定するには、ユーザ名 webvpn コンフィギュレーション モードで **username attributes** コマンドを入力してから、**webvpn** コマンドを入力します。詳細については **webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）を参照してください。

例

次に、「anyuser」という名前のユーザのユーザ名属性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。

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)#
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	ASA データベースにユーザを追加します。
webvpn	webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

username-from-certificate

認可のためのユーザ名として、証明書内のいずれのフィールドを使用するかを指定するには、トンネル グループ一般属性モードで **username-from-certificate** コマンドを使用します。認可のためのユーザ名として使用するピア証明書の DN。

属性をコンフィギュレーションから削除して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。

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

構文の説明

primary-attr	証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
secondary-attr	(任意)デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
use-entire-name	ASA では、完全なサブジェクト DN(RFC1779)を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。
use-script	ASDM によって生成されたスクリプト ファイルを使用して、ユーザ名として使用する DN フィールドを証明書から抽出することを指定します。

デフォルト

プライマリ属性のデフォルト値は CN(一般名)です。

セカンダリ属性のデフォルト値は OU(組織の部門)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	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

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

このコマンドは、ユーザ名として使用する証明書内のフィールドを選択します。このコマンドは、リリース 8.0(4) 以降で廃止された **authorization-dn-attributes** コマンドに代わるものです。**username-from-certificate** コマンドは、セキュリティ アプライアンスに、指定した証明書フィールドをユーザ名/パスワード認可のためのユーザ名として使用するように強制します。

ユーザ名/パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたこのユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドも設定する必要があります。つまり、ユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。
use-script	ASDM によって生成されたスクリプト ファイルを使用します。

例

グローバル コンフィギュレーション モードで入力される次の例では、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成して、Common Name（CN; 通常名）をプライマリ属性として使用し、認可クエリー用の名前をデジタル証明書から生成するために使用するセカンダリ属性として OU を使用することを指定します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN OU
ciscoasa(config-tunnel-general)#
```

次に、トンネル グループ属性を変更し、事前入力ユーザ名を設定する例を示します。

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

username-from-certificate-choice

プライマリ認証または許可用として事前入力ユーザ名フィールドにユーザ名を使用する必要がある証明書を選択するには、**username-from-certificate-choice** コマンドを使用します。このコマンドは tunnel-group general-attributes モードで使用します。デフォルトの証明書で使用されているユーザ名を使用するには、このコマンドの **no** 形式を使用します。

username-from-certificate-choice {**first-certificate** | **second-certificate**}

no username-from-certificate-choice {**first-certificate** | **second-certificate**}

構文の説明

first-certificate	マシン証明書のユーザ名を、プライマリ認証の事前入力ユーザ名フィールドで使用するように SSL または IKE で送信するかどうかを指定します。
second-certificate	ユーザ証明書のユーザ名を、プライマリ認証の事前入力ユーザ名フィールドで使用するようにクライアントから送信するかどうかを指定します。

デフォルト

デフォルトでは、事前入力するユーザ名は 2 つ目の証明書から取得されます。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

複数証明書オプションを使用すると、証明書を通じたマシンとユーザ両方の証明書認証が可能になります。事前入力ユーザ名フィールドでは、証明書のフィールドを解析し、AAA および証明書認証済み接続で以降の（プライマリまたはセカンダリ）AAA 認証に使用することができます。事前入力のユーザ名は、常にクライアントから受信した 2 つ目の（ユーザ）証明書から取得されます。

9.14(1) 以降、ASA では、最初の証明書（マシン証明書）または 2 つ目の証明書（ユーザ証明書）のどちらを使用して事前入力ユーザ名フィールドに使用するユーザ名を取得するかを選択できます。

このコマンドは、認証タイプ（AAA、証明書、または複数証明書）に関係なく、任意のトンネルグループに使用および設定できます。ただし、設定は、複数証明書認証（複数証明書または AAA 複数証明書）に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2 つ目の証明書がデフォルトとして認証または許可の目的で使用されます。

例

次に、プライマリおよびセカンダリ認証または許可の事前入力ユーザ名に使用する証明書を設定する方法の例を示します。

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>
ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice
first-certificate

ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

関連コマンド

コマンド	説明
secondary-username-from-certificate-choice	セカンダリ認証の証明書オプションを指定します。

username password-date

システムがブート時または実行コンフィギュレーションへのファイルのコピー時にパスワード作成日付を復元できるようにするには、非インタラクティブ コンフィギュレーション モードで **username pasword-date** コマンドを入力します。言い換えると、このコマンドは、このコマンドがすでに存在しているときにコンフィギュレーション ファイルをブート アップする場合にのみ使用できます。CLI プロンプトにこのコマンドを入力することはできません。

username *name* **password-date** *date*

構文の説明

name	3 ～ 64 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字を使用して、ユーザ名を指定します。
date	ブートアップ時にユーザ名が読み込まれるときに、システムがパスワード作成日付を復元できるようにします。存在しない場合、パスワード日付は現在の日付に設定されます。日付の形式は、mmm-dd-yyyy です。

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	トランスペアレント	シングル	コンテキスト	システム
非インタラクティブ	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザ名パスワード日付を表示するには、**show running-config all username** コマンドを使用します。

CLI プロンプトから **username password-date** 値を入力することはできません。パスワード日付は、パスワード ポリシーの有効期間がゼロでない場合にだけスタートアップ コンフィギュレーションに保存されます。これは、パスワードの有効期限が設定されている場合に限り、パスワード日付が保存されることを意味します。ユーザがパスワード作成日を変更することを防ぐために **username password-date** コマンドを使用することはできません。

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのユーザ名プロンプトをカスタマイズするには、Webvpn カスタマイゼーション モードで **username-prompt** 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して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

ユーザ名プロンプトのデフォルト テキストは「USERNAME:」です。

ユーザ名プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right 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	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、テキストを「Corporate Username:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# username-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# username-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。

validate-attribute コマンド～ vxlan port コマンド

validate-attribute

RADIUS アカウンティングの使用時に RADIUS 属性を検証するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **validate-attribute** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

構文の説明

attribute_number	RADIUS アカウンティングで検証する RADIUS 属性。値の範囲は、1 ～ 191 です。ベンダー固有属性はサポートされません。

デフォルト

このオプションは、デフォルトで無効です。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを設定すると、セキュリティ アプライアンスは、Framed IP 属性に加えて RADIUS 属性に対する照合も実行します。このコマンドは、インスタンスを複数設定できます。

RADIUS 属性のタイプのリストを見るには、次のサイトにアクセスしてください。

http://www.iana.org/assignments/radius-types

例

次に、ユーザ名 RADIUS 属性の RADIUS アカウンティングをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate-attribute 1
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

validate-kdc

アップロードされたキータブファイルを使用した Kerberos キー発行局（KDC）の認証を有効にするには、AAA サーバグループモードで **validate-kdc** コマンドを使用します。KDC 認証を無効にするには、このコマンドの **no** 形式を使用します。

validate-kdc

no validate-kdc

デフォルト

このオプションは、デフォルトで無効です。

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバグループ	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(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

validate-kdc コマンドを使用して、グループ内のサーバを認証するように Kerberos AAA サーバグループを設定できます。認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザクレデンシャルが攻撃者の Kerberos サーバに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット（TGT）を取得してユーザを検証した後、システムは **ホスト/***ASA_hostname* のユーザに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバは信頼できないと見なされ、ユーザは認証されません。

KDC 認証を完了するには、次の手順を実行する必要があります。

1. （KDC 上。）ASA の Microsoft Active Directory でユーザアカウントを作成します（[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] に移動します）。たとえば、ASA の完全修飾ドメイン名（FQDN）が asahost.example.com の場合は、asahost という名前のユーザを作成します。
2. （KDC 上。）FQDN とユーザアカウントを使用して、ASA のホストサービスプリンシパル名（SPN）を作成します。

```
C:> setspn -A HOST/asahost.example.com asahost
```

3. （KDC 上。）ASA の キータブファイルを作成します（わかりやすくするために改行を追加）。

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

4. （ASA 上。）**aaa kerberos import-keytab** コマンドを使用して、キータブ（この例では new.keytab）を ASA にインポートします。
5. （ASA 上。）Kerberos AAA サーバグループ設定に **validate-kdc** コマンドを追加します。キータブファイルは、このコマンドが含まれているサーバグループでのみ使用されます。

（注） Kerberos 制約付き委任（KCD）とともに KDC 検証を使用することはできません。サーバグループが KCD に使用されている場合、**validate-kdc** コマンドは無視されます。

例

次に、FTP サーバ上に存在する new.keytab というキータブをインポートし、Kerberos AAA サーバグループで KDC 検証を有効にする例を示します。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

関連コマンド

コマンド	説明
aaa kerberos import-keytab	Kerberos キー発行局（KDC）からエクスポートされた Kerberos キータブファイルをインポートします。
clear aaa kerberos keytab	インポートされた Kerberos キータブファイルをクリアします。
show aaa kerberos keytab	Kerberos キータブファイルに関する情報を表示します。

validate-key

LISP メッセージの事前共有キーを指定するには、パラメータ コンフィギュレーション モードで **validate-key** 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 モードにアクセスするには、まず **policy-map type inspect lisp** コマンドを入力します。キーを削除するには、このコマンドの **no** 形式を使用します。

validate-key *key*

no validate-key *key*

構文の説明

key	LISP メッセージの事前共有キーを指定します。

コマンド 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が LISP メッセージの内容を読み取ることができるように、LISP 事前共有キーを指定します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、EID を 10.10.10.0/24 ネットワーク上に制限して、事前共有キーを指定する例を示します。

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。

コマンド	説明
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。

validation-policy

着信ユーザ接続に関連付けられている証明書を検証するためにトラストポイントを使用できる条件を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-policy** コマンドを使用します。指定した条件でトラストポイントを使用できないように指定するには、このコマンドの **no** 形式を使用します。

[no] validation-policy {ssl-client | ipsec-client} [no-chain] [subordinate-only]

構文の説明

ipsec-client	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを IPsec 接続の検証に使用できることを指定します。
no-chain	セキュリティ デバイス上にない下位証明書のチェーンをディセーブルにします。
ssl-client	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。
subordinate-only	このトラストポイントで表される CA から直接発行されたクライアント証明書の検証をディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

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。

コマンド履歴

	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	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

リモート アクセス VPN では、導入要件に応じて、セキュア ソケット レイヤ（SSL）VPN、IP Security（IPsec）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。**validation-policy** コマンドを使用して、オンボード CA 証明書へのアクセスに使用できるプロトコル タイプを指定できます。

このコマンドで **no-chain** オプションを指定すると、ASA でトラストポイントとして設定されていない下位 CA 証明書が ASA でサポートされなくなります。

ASA では、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能がイネーブルになっている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントが指定したトラストポイントの下位証明書を受け入れるように設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

validation-usage

このトラストポイントでの検証が許可される使用タイプを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **validation-usage** コマンドを使用します。使用タイプを指定しない場合は、このコマンドの **no** 形式を使用します。

validation-usage ipsec-client | ssl-client | ssl-server

no validation-usage ipsec-client | ssl-client | ssl-server

構文の説明

ipsec-client	このトラストポイントを使用して IPsec クライアント接続を検証できることを示します。
ssl-client	このトラストポイントを使用して SSL クライアント接続を検証できることを示します。
ssl-server	このトラストポイントを使用して SSL サーバ証明書を検証できることを示します。

デフォルト

ipsec-client、ssl-client

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	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	client-types コマンドを置き換える目的でこのコマンドが追加されました。

使用上のガイドライン

同じ CA 証明書に関連付けられているトラストポイントが複数ある場合、特定のクライアント タイプに設定できるのは 1 つのトラストポイントだけです。ただし、1 つのトラストポイントを 1 つのクライアント タイプに設定し、別のトラストポイントを別のクライアント タイプに設定することができます。

同じ CA 証明書に関連付けられているトラストポイントがあり、これがすでに 1 つのクライアント タイプに設定されている場合は、この同じクライアント タイプ設定に新しいトラストポイントを設定することはできません。このコマンドの **no** 形式を使用して設定をクリアして、トラストポイントがいずれのクライアント検証にも使用できないようにすることができます。

リモート アクセス VPN では、配置の要件に応じて、セキュア ソケット レイヤ（SSL）VPN、IP Security（IPsec）、またはこの両方を使用して、すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

vdi

モバイル デバイスで実行される Citrix Receiver アプリケーションの XenDesktop および XenApp VDI サーバへのセキュアなリモート アクセスを ASA 経由で提供するには、**vdi** コマンドを使用します。

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

構文の説明

domain *domain*	仮想化インフラストラクチャ サーバにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
password *password*	仮想化インフラストラクチャ サーバにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。
type	VDI のタイプ。Citrix Receiver タイプの場合、この値は *citrix* にする必要があります。
url *url*	http または https、ホスト名、ポート番号、および XML サービスへのパスを含む XenApp または XenDesktop サーバの完全な URL。
username *username*	仮想化インフラストラクチャ サーバにログインするためのユーザ名。この値は、クライアントレス マクロにすることができます。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

VDI モデルでは、管理者は、企業アプリケーションが事前にロードされているデスクトップをパブリッシュし、エンド ユーザは、これらのデスクトップにリモート アクセスします。これらの仮想リソースは、ユーザが Citrix Access Gateway を移動してアクセスする必要がないように、電子メールなどのその他のリソースと同様に表示されます。ユーザは Citrix Receiver モバイル クライアントを使用して ASA にログオンし、ASA は事前定義された Citrix XenApp または XenDesktop サーバに接続されます。ユーザが Citrix の仮想化されたリソースに接続する場合に、Citrix サーバのアドレスおよびクレデンシャルをポイントするのではなく、ASA の SSL VPN IP アドレスおよびクレデンシャルを入力するように、管理者は [Group Policy] で Citrix サーバのアドレスおよびログオン クレデンシャルを設定する必要があります。ASA がクレデンシャルを確認したら、受信側クライアントは ASA 経由で許可されているアプリケーションの取得を開始します。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x 電話機：Citrix Receiver バージョン 2.x 以降
- Android 3.x タブレット：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

例

ユーザ名とグループ ポリシーが両方とも設定されている場合、ユーザ名の設定は、グループ ポリシーに優先します。

```
configure terminal
    group-policy DfltGrpPolicy attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>
configure terminal
    username <username> attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>]
```

関連コマンド

コマンド	説明
debug webvpn citrix	Citrix ベースのアプリケーションおよびデスクトップを起動するプロセスの状況を知ることができます。

verify

ファイルのチェックサムを確認するには、特権 EXEC モードで **verify** コマンドを使用します。

verify *path*

verify {**/md5** | **sha-512**} *path* [*expected_value*]

verify /signature running

構文の説明

/md5	指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
/sha-512	指定したソフトウェア イメージの SHA-512 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
/signature running	実行中の ASA イメージの署名を確認します。

expected_value	(オプション)指定したイメージの既知のハッシュ値。ハッシュ値が一致するか、または不一致があるかどうかを確認するメッセージが ASA に表示されます。
path	• **disk0:/**[*path*/]*filename* 内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:/**[*path*/]*filename* 外部フラッシュ メモリ カードを示します。 • **flash:/**[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。**flash** は **disk0:** のエイリアスです。 • **ftp://**[*user*[**:***password*]@]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**:ASCII 受動モード – **an**:ASCII 通常モード – **ip**:(デフォルト)バイナリ受動モード – **in**:バイナリ通常モード • **http**[**s**]**://**[*user*[**:***password*]@]*server*[:*port*]/[*path*/]*filename* • **tftp://**[*user*[**:***password*]@]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**verify** コマンドではなく **tftp-server** コマンドでパスを設定します。 • **system:running-config** 実行コンフィギュレーションのハッシュを計算するか、または確認します。 • **system:text** ASA プロセスのテキストのハッシュを計算するか、または確認します。

デフォルト

現在のフラッシュ デバイスがデフォルトのファイル システムです。

(注) **/md5** または **/sha-512** オプションを指定する場合、FTP、HTTP、TFTP などのネットワーク ファイルをソースとして使用できます。**/md5** または **/sha-512** オプションを指定せずに **verify** コマンドを使用した場合は、フラッシュのローカル イメージのみを確認できます。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.3(2)	**signature** キーワードが追加されました。
9.6(2)	**system:text** オプションが追加されました。

使用上のガイドライン

verify コマンドを使用して、ファイルを使用する前にそのチェックサムを確認します。

ディスクで配布される各ソフトウェア イメージでは、イメージ全体に対して 1 つのチェックサムが使用されます。このチェックサムは、イメージをフラッシュ メモリにコピーする場合にのみ表示され、イメージ ファイルをあるディスクから別のディスクにコピーする場合は表示されません。

新しいイメージをロードまたは複製する前に、そのイメージのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリまたはサーバにコピーするときにチェックサムを確認できるようにします。Cisco.com では、さまざまなイメージ情報を入手できます。

フラッシュ メモリの内容を表示するには、**show flash** コマンドを使用します。フラッシュ メモリの内容のリストには、個々のファイルのチェックサムは含まれません。イメージをフラッシュ メモリにコピーした後で、そのイメージのチェックサムを再計算して確認するには、**verify** コマンドを使用します。ただし、**verify** コマンドでは、ファイルがファイル システムに保存された後にのみ、整合性チェックを実行します。破損しているイメージが ASA に転送され、検出されずにファイル システムに保存される場合があります。破損しているイメージが正常に ASA に転送されると、ソフトウェアはイメージが壊れていることを把握できず、ファイルの確認が正常に完了します。

メッセージ ダイジェスト 5（MD5）ハッシュ アルゴリズムを使用してファイルを検証するには、**/md5** オプションを指定して **verify** コマンドを使用します。MD5（RFC 1321 で規定）は、一意の 128 ビットのメッセージ ダイジェストを作成することによってデータ整合性を確認するアルゴリズムです。**verify** コマンドの **/md5** オプションを使用すると、ASA ソフトウェア イメージの MD5 チェックサム値を、その既知の MD5 チェックサム値と比較することによって、イメージの整合性を確認できます。すべてのセキュリティ アプライアンスのソフトウェア イメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。SHA-512（**/sha-512**）を指定することもできます。

MD5 または SHA-512 整合性チェックを行うには、**/md5** または **/sha-512** キーワードを使用して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェア イメージの MD5 値が計算され、表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、まず Cisco.com から MD5 値を取得し、その値をコマンド構文で指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しない場合は、いずれかのイメージが破損しているか、または入力した MD5 値が正しくありません。

例

次に、cdisk.bin というイメージ ファイルに対して使用された **verify** コマンドの例を示します。わかりやすくするために、一部のテキストは省略されています。

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

次に、disk0 の署名イメージに対して使用された **verify** コマンドの例を示します。

```
ciscoasa(config)# verify lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6

Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6


Digital signature successfully validate

ciscoasa(config)# verify /signature lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6

Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6


Digital signature successfully validated
ciscoasa(config)# verify /signature cdisk.smp
Verifying file integrity of disk0:/cdisk.smp
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!Done!
Embedded Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
```

```
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f0599
7fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

verify-header

既知の IPv6 拡張ヘッダーだけを許可し、IPv6 拡張ヘッダーの順序を適用するには、パラメータ コンフィギュレーション モードで **verify-header** コマンドを適用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect ipv6** コマンドを入力します。これらのパラメータを無効にするには、このコマンドの **no** 形式を使用します。

verify-header {**order** | **type**}

no verify-header {**order** | **type**}

構文の説明

order	RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。
type	既知の IPv6 拡張ヘッダーのみを許可します。

コマンド デフォルト

順序とタイプの両方がデフォルトでイネーブルになります。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

これらのパラメータは、デフォルトでイネーブルになっています。ディセーブルにするには、no キーワードを入力します。

例

次の例では、IPv6 インスペクション ポリシー マップの order および type パラメータをディセーブルにします。

```
ciscoasa(config)# policy-map type inspect ipv6 ipv6-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# no verify-header order
ciscoasa(config-pmap-p)# no verify-header type
```

関連コマンド

コマンド	説明
inspect ipv6	IPv6 インスペクションをイネーブルにします。
parameters	インスペクション ポリシー マップのパラメータ コンフィギュレーション モードを開始します。
policy-map type inspect ipv6	IPv6 インスペクション ポリシー マップを作成します。

version

ASA でグローバルに使用する RIP のバージョンを指定するには、ルータ コンフィギュレーション モードで **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

ASA は、バージョン 1 およびバージョン 2 のパケットを受信しますが、送信するのはバージョン 1 のパケットのみです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを入力することによって、インターフェイスごとにグローバルな設定を上書きすることができます。

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、すべてのインターフェイスで RIP バージョン 2 のパケットを送受信するように ASA を設定する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 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。
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。

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバ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。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

構文の説明

ip_address	ASA 上の仮想 HTTP サーバの IP アドレスを設定します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。
warning	（任意）HTTP 接続 を ASA にリダイレクトする必要があることをユーザに通知します。このキーワードは、リダイレクトが自動的に行われないテキストベースのブラウザにのみ適用されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	以前のリリースで使用されていたインライン基本 HTTP 認証方式がリダイレクション方式に置き換えられたため、このコマンドは廃止され、不要になりました。
7.2(2)	**aaa authentication listener** コマンドを使用して、基本 HTTP 認証（デフォルト）と HTTP リダイレクションのいずれを使用するかを選択できるようになったため、このコマンドは復活しました。リダイレクション方式では、HTTP 認証をカスケードするための特別なコマンドは必要ありません。

使用上のガイドライン

ASA で HTTP 認証を使用する場合は（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、ASAで基本 HTTP 認証がデフォルトで使用されます。**redirect** キーワードを指定した **aaa authentication listener** を使用して、ASA が HTTP 接続を ASA によって生成された Web ページにリダイレクトするように認証方式を変更できます。

ただし、基本 HTTP 認証の使用を続行する場合は、HTTP 認証をカスケードするときに **virtual http** コマンドが必要になることがあります。

ASA に加えて宛先 HTTP サーバで認証が必要な場合は、**virtual http** コマンドを使用して、ASA（AAA サーバ経由）と HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、ASA に対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

このコマンドは、AAA 認証を必要とするすべての HTTP 接続を ASA 上の仮想 HTTP サーバにリダイレクトします。ASA により、AAA サーバのユーザ名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバがユーザを認証すると、ASA は HTTP 接続を元のサーバにリダイレクトして戻しますが、AAA サーバのユーザ名とパスワードは含めません。HTTP パケットにユーザ名とパスワードが含まれていないため、HTTP サーバによりユーザに HTTP サーバのユーザ名とパスワードの入力を求めるプロンプトが別途表示されます。

着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 HTTP アドレスも含める必要があります。さらに、NAT が必要ない場合でも（**no nat-control** コマンドを使用）、仮想 HTTP IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます（アドレスを同一アドレスに変換）。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

（注） **virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの期間を 0 秒に設定しないでください。設定すると、実際の Web サーバへの HTTP 接続ができなくなります。

例

次に、AAA 認証とともに仮想 HTTP をイネーブルにする例を示します。

```
ciscoasa(config)# virtual http 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list ACL-IN remark This is the HTTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list ACL-IN remark This is the virtual HTTP address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list AUTH remark This is the HTTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list AUTH remark This is the virtual HTTP address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
aaa authentication listener http	ASA が認証に使用する方式を設定します。
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	ASA 仮想サーバの IP アドレスを表示します。
sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにする場合は、このコマンドを使用すると、ブラウザ キャッシュ内のユーザ名とパスワードを使用して仮想サーバに再接続できます。
virtual telnet	ASA 上に仮想 Telnet サーバを設定して、認証を必要とする他のタイプの接続を開始する前に、ユーザを ASA で認証できるようにします。

virtual telnet

ASA 上に仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。ASA によって認証プロンプトが表示されない他のタイプのトラフィックに対する認証が必要な場合は、仮想 Telnet サーバでユーザを認証する必要があります。サーバ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。

virtual telnet *ip_address*

no virtual telnet *ip_address*

構文の説明

ip_address	ASA 上の仮想 Telnet サーバの IP アドレスを設定します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

任意のプロトコルまたはサービスのネットワーク アクセス認証を設定できますが（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、HTTP、Telnet、または FTP のみで直接認証することもできます。ユーザがまずこれらのサービスのいずれかで認証を受けておかないと、他のサービスは通過を許可されません。HTTP、Telnet、または FTP の ASA の通過を許可せず、その他のタイプのトラフィックを認証する場合は、ASA 上で設定された所定の IP アドレスにユーザが Telnet で接続し、ASA によって Telnet プロンプトが表示されるように、仮想 Telnet を設定できます。

authentication match コマンドまたは **aaa authentication include** コマンドを使用して、仮想 Telnet アドレスおよび認証するその他のサービスへの Telnet アクセスに対する認証を設定する必要があります。

認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを求められ、その後 AAA サーバにより認証されます。認証されると、ユーザに [Authentication Successful.] というメッセージが表示されます。これで、ユーザは認証が必要な他のサービスにアクセスできます。

着信ユーザ(セキュリティの低い方から高い方へ向かう)については、送信元インターフェイスに適用されるアクセス リストに宛先インターフェイスとして仮想 Telnet アドレスも含める必要があります。さらに、NAT が必要ない場合でも(**no nat-control** コマンドを使用)、仮想 Telnet IP アドレスに対する **static** コマンドを追加する必要があります。通常、アイデンティティ NAT コマンドが使用されます(アドレスを同一アドレスに変換)。

発信ユーザについては、トラフィックの許可は明示的に行われますが、内部インターフェイスにアクセス リストを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可してください。**static** ステートメントは不要です。

ASA からログアウトするには、仮想 Telnet IP アドレスに再接続します。ログアウトするように求められます。

例

次に、他のサービスに対する AAA 認証とともに仮想 Telnet をイネーブルにする例を示します。

```
ciscoasa(config)# virtual telnet 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list ACL-IN remark This is the SMTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
ciscoasa(config)# access-list ACL-IN remark This is the virtual Telnet address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list AUTH remark This is the SMTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list AUTH remark This is the virtual Telnet address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド ステートメントを削除します。
show running-config virtual	ASA 仮想サーバの IP アドレスを表示します。
virtual http	ASA 上で HTTP 認証を使用し、HTTP サーバも認証を要求する場合は、このコマンドを使用して、ASA と HTTP サーバで別々に認証を受けることができます。仮想 HTTP を使用しない場合は、ASA に対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

vlan（グループポリシー）

VLAN をグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで **vlan** コマンドを使用します。グループ ポリシーのコンフィギュレーションから VLAN を削除し、デフォルトのグループ ポリシーの VLAN 設定に置き換えるには、このコマンドの **no** 形式を使用します。

[**no**] **vlan** {*vlan_id* |**none**}

構文の説明

none	このグループ ポリシーに一致するリモート アクセス VPN セッションへの VLAN の割り当てをディセーブルにします。グループ ポリシーは、デフォルトのグループ ポリシーから vlan 値を継承しません。
vlan_id	このグループ ポリシーを使用するリモート アクセス VPN セッションに割り当てる VLAN の番号（10 進表記）。インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用して、この ASA に VLAN を設定する必要があります。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、このグループ ポリシーに割り当てられているセッションの出力 VLAN インターフェイスを指定します。ASA は、このグループのすべてのトラフィックを指定された VLAN に転送します。VLAN を各グループ ポリシーに割り当ててアクセス コントロールを簡素化できます。このコマンドは、セッション上のトラフィックをフィルタリングする ACL の代わりに使用します。

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、VLAN マッピング オプションでは使用しないでください。vlan-mapping 設定によってパケットが間違ってルーティングされる可能性があるため、これらのインスペクション エンジンは、vlan-mapping 設定を無視します。

例

次のコマンドでは、VLAN 1 をグループ ポリシーに割り当てます。

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

次のコマンドでは、VLAN マッピングをグループ ポリシーから削除します。

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
show vlan	ASA に設定されている VLAN を表示します。
vlan（インターフェイス コンフィギュレーション モード）	サブインターフェイスに VLAN ID を割り当てます。
show vpn-session_summary.db	IPsec、Cisco AnyConnect、NAC の各セッションの数および使用中の VLAN の数を表示します。
show vpn-sessiondb	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

vlan（インターフェイス）

VLAN ID をサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスでは、トラフィックを通過させるために VLAN ID が必要です。VLAN サブインターフェイスを使用して、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLAN を使用すると、所定の物理インターフェイス上で複数のセキュリティ コンテキストなどのトラフィックを別々に保管できます。

vlan *id* [**secondary** *vlan_range*]

no vlan [**secondary** *vlan_range*]

構文の説明

id	1 ～ 4094 の範囲の整数を指定します。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。
secondary *vlan_range*	（オプション）1 つまたは複数のセカンダリ VLAN を指定します。*vlan_id* は、1 ～ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。 セカンダリ VLAN は、（連続する範囲について）スペース、カンマ、およびダッシュで区切ることができます。ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。
9.5(2)	**secondary** キーワードが追加されました。

使用上のガイドライン

1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN を設定できます。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。リストからいくつかのセカンダリ VLAN を削除するには、**no** コマンドを使用して削除する VLAN のみをリストすることができます。リストされた VLAN のみを選択的に削除できます。たとえば、範囲内の 1 つの VLAN を削除することはできません。

サブインターフェイスをイネーブルにするには、**no shutdown** コマンドを使用して物理インターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。したがって、インターフェイスを停止することによって物理インターフェイスを介したトラフィックの通過を防止することはできません。代わりに、**nameif** コマンドを省略することによって、トラフィックが物理インターフェイスを通過しないようにします。物理インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって異なります。プラットフォームごとのサブインターフェイスの最大数については、CLI 設定ガイドを参照してください。

例

次に、VLAN 101 をサブインターフェイスに割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、VLAN を 102 に変更する例を示します。

```
ciscoasa(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-interface)# vlan 102

ciscoasa(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

次に、一連のセカンダリ VLAN を VLAN 200 にマップする例を示します。

```
interface gigabitethernet 0/6.200
    vlan 200 secondary 500 503 600-700
```

次に、リストからセカンダリ VLAN 503 を削除する例を示します。

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
    vlan 200 secondary 500 600-700
    no nameif
    no security-level
    no ip address
```

次に、Catalyst 6500 でどのように VLAN マッピングが機能するのかを示します。ノードを PVLANS に接続する方法については、Catalyst 6500 の設定ガイドを参照してください。

ASA の設定

```
interface GigabitEthernet1/1
      description Connected to Switch GigabitEthernet1/5
      no nameif
      no security-level
      no ip address
      no shutdown
!
interface GigabitEthernet1/1.70
      vlan 70 secondary 71 72
      nameif vlan_map1
      security-level 50
      ip address 10.11.1.2 255.255.255.0
      no shutdown
!
interface GigabitEthernet1/2
      nameif outside
      security-level 0
      ip address 172.16.171.31 255.255.255.0
      no shutdown
```

Catalyst 6500 の設定

```
vlan 70
      private-vlan primary
      private-vlan association 71-72
!
vlan 71
      private-vlan community
!
vlan 72
      private-vlan isolated
!
interface GigabitEthernet1/5
      description Connected to ASA GigabitEthernet1/1
      switchport
      switchport trunk encapsulation dot1q
      switchport trunk allowed vlan 70-72
      switchport mode trunk
!
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vpdn group

VPDN グループを作成または編集し、PPPoE クライアントを設定するには、グローバル コンフィギュレーション モードで **vpdn group** コマンドを使用します。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

vpdn group *group_name* {**localname** *username* | **request dialout pppoe** | **ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** *name* | **request dialout pppoe** | **ppp authentication** {**chap** | **mschap** | **pap**}}

(注) PPPoE は、ASA でフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

localname *username*	ユーザ名を認証のために VPDN グループにリンクし、**vpdn username** コマンドで設定された名前と照合する必要があります。
**ppp authentication {chap | mschap | pap}}	ポイントツーポイント プロトコル（PPP）認証プロトコルを指定します。Windows クライアントのダイヤルアップ ネットワーク設定を使用して、使用する認証プロトコル（PAP、CHAP、または MS-CHAP）を指定できます。クライアントで指定した設定は、セキュリティ アプライアンスで使用する設定と一致している必要があります。パスワード認証プロトコル（PAP）を使用すると、PPP ピアは相互に認証できます。PAP は、ホスト名またはユーザ名をクリアテキストで渡します。チャレンジ ハンドシェイク認証プロトコル（CHAP）を使用すると、PPP ピアは、アクセス サーバとの通信によって不正アクセスを防止できます。MS-CHAP は Microsoft 版の CHAP です。PIX Firewall では、MS-CHAP バージョン 1 のみサポートされます（バージョン 2.0 はサポートされません）。 ホストで認証プロトコルが指定されていない場合は、コンフィギュレーションで **ppp authentication** オプションを指定しないでください。
request dialout pppoe	ダイヤルアウト PPPoE 要求を許可することを指定します。
vpdn group *group_name*	VPDN グループ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	トランスペアレント	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	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

バーチャル プライベート ネットワーク（VPDN）は、リモート ダイヤルイン ユーザとプライベート ネットワーク間の長距離のポイントツーポイント接続を提供するために使用します。セキュリティ アプライアンス上の VDPN では、レイヤ 2 トンネリング技術の PPPoE を使用して、リモート ユーザからパブリック ネットワーク経由のプライベート ネットワークへのダイヤルアップ ネットワーク接続を確立します。

PPPoE は、Point-to-Point Protocol（PPP）over Ethernet です。PPP は、IP、IPX、ARA などのネットワーク層プロトコルで動作するように設計されています。PPP には、セキュリティ メカニズムとして CHAP と PAP も組み込まれています。

PPPoE 接続のセッション情報を表示するには、**show vpdn session pppoe** コマンドを使用します。コンフィギュレーションからすべての **vpdn group** コマンドを削除して、すべてのアクティブな L2TP トンネルと PPPoE トンネルを停止するには、**clear configure vpdn group** コマンドを使用します。**clear configure vpdn username** コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

PPPoE は PPP をカプセル化するため、PPPoE は PPP を使用して、認証および VPN トンネル内で動作しているクライアント セッションに対する ECP 機能と CCP 機能を実行します。さらに、PPP によって PPPoE に IP アドレスが割り当てられるため、PPPoE と DHCP の併用はサポートされません。

（注）　PPPoE に VPDN グループが設定されていない場合、PPPoE は接続を確立できません。

PPPoE に使用する VPDN グループを定義するには、**vpdn group** *group_name* **request dialout pppoe** コマンドを使用します。次に、インターフェイス コンフィギュレーション モードで **pppoe client vpdn group** コマンドを使用して、VPDN グループを特定のインターフェイス上の PPPoE クライアントに関連付けます。

ISP が認証を要求している場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドを使用して、ISP で使用される認証プロトコルを選択します。

ISP によって割り当てられたユーザ名を VPDN グループに関連付けるには、**vpdn group** *group_name* **localname** *username* コマンドを使用します。

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、**vpdn username** *username* password *password* コマンドを使用します。ユーザ名は、PPPoE に指定した VPDN グループにすでに関連付けられているユーザ名にする必要があります。

(注) ISP で CHAP または MS-CHAP が使用されている場合、ユーザ名はリモート システム名、パスワードは CHAP シークレットと呼ばれることがあります。

PPPoE クライアント機能はデフォルトでオフになっているため、VPDN の設定後、**ip address** *if_name* **pppoe** [**setroute**] コマンドを使用して PPPoE をイネーブルにします。**setroute** オプションを指定すると、デフォルト ルートが存在しない場合にデフォルト ルートが作成されます。

PPPoE の設定後すぐに、セキュリティ アプライアンスは通信する PPPoE アクセス コンセントレータを探します。PPPoE 接続が正常終了または異常終了すると、ASA は通信する新しいアクセス コンセントレータを探します。

次の **ip address** コマンドは、PPPoE セッションの開始後に使用しないでください。使用すると、PPPoE セッションが終了します。

- **ip address outside pppoe**: このコマンドは新しい PPPoE セッションを開始しようとします。
- **ip address outside dhcp**: このコマンドは、インターフェイスがその DHCP 設定を取得するまでインターフェイスをディセーブルにします。
- **ip address outside** *address netmask*: インターフェイスが正常に初期化されたインターフェイスとして起動するため。

例

次に、VDPN グループ *telecommuters* を作成し、PPPoE クライアントを設定する例を示します。

```
ciscoasa(config)# vpdn group telecommuters request dialout pppoe
ciscoasa(config)# vpdn group telecommuters localname user1
ciscoasa(config)# vpdn group telecommuters ppp authentication pap
ciscoasa(config)# vpdn username user1 password test1
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-subif)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group *group_name*	VPDN グループのコンフィギュレーションを表示します。
vpdn username	PPPoE 接続用のユーザ名とパスワードのペアを作成します。

vpdn username

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、グローバル コンフィギュレーション モードで **vpdn username** コマンドを使用します。

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

(注) PPPoE は、ASA でフェールオーバーを設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

構文の説明

password	パスワードを指定します。
store-local	ユーザ名とパスワードをセキュリティ アプライアンス上の NVRAM の特別な場所に保存します。Auto Update Server が clear config コマンドをセキュリティ アプライアンスに送信し、接続が中断されると、セキュリティ アプライアンスは NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再認証できます。
username	ユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。「使用上のガイドライン」を参照してください。

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	トランスペアレント	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	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

VPDN ユーザ名は、**vpdn group** *group_name* **localname** *username* コマンドで指定された VPDN グループにすでに関連付けられているユーザ名にする必要があります。

clear configure vpdn username コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

例

次に、パスワードが *telecommuter*9/8 の *bob_smith* という VPDN ユーザ名を作成する例を示します。

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての **vpdn group** コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての **vpdn username** コマンドをコンフィギュレーションから削除します。
show vpdn group	VPDN グループのコンフィギュレーションを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

vpn-access-hours

グループ ポリシーを設定済み time-range ポリシーに関連付けるには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** 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。このオプションを使用すると、他のグループ ポリシーから time-range 値を継承できます。値が継承されないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

構文の説明

none	VPN アクセス時間をヌル値に設定して、time-range ポリシーを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

デフォルト

制限なし。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、FirstGroup というグループ ポリシーを 824 という time-range ポリシーに関連付ける例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日と 1 日の時間を設定します(開始日と終了日を含む)。

vpn-addr-assign

IPv4 アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。設定されている VPN アドレスの割り当て方法を ASA からすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *delay*]}

構文の説明

aaa	外部または内部（ローカル）AAA 認証サーバから IPv4 アドレスを割り当てます。
dhcp	DHCP 経由で IP アドレスを取得します。
ローカル	ASA に設定されている IP アドレス プールから IP アドレスを割り当てて、トンネル グループに関連付けます。
reuse-delay *delay*	解放された IP アドレスを再利用するまでの遅延時間。指定できる範囲は 0 ～ 480 分です。デフォルトは 0（ディセーブル）です。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(3)	**reuse-delay** オプションが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバが使用できる IP アドレスの範囲も定義する必要があります。DHCP サーバが使用する IP アドレスを指定するには、**dhcp-server** コマンドを使用する必要があります。

ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。次に、**vpn-framed-ip-address** コマンドと **vpn-framed-netmask** コマンドを使用して、IP アドレスとネットマスクを個々のユーザに割り当てます。

ローカル プールを使用する場合は、**reuse-delay** *delay* オプションを使用して、解放された IP アドレスを再利用するまでの遅延時間を調整します。遅延時間を長くすると、IP アドレスがプールに戻されて即座に再割り当てされるときにファイアウォールで発生する可能性がある問題を回避できます。

AAA を選択する場合は、設定済みのいずれかの RADIUS サーバから IP アドレスを取得します。

例

次に、アドレス割り当て方法として DHCP を設定する例を示します。

```
ciscoasa(config)# vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	ASA DHCP サーバがグループ ポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲を指定します。
ip-local-pool	ローカル IP アドレス プールを作成します。
ipv6-addr-assign	リモート アクセス クライアントに IPv6 アドレスを割り当てる方法を指定します。
vpn-framed-ip-address	特定のユーザに割り当てる IP アドレスを指定します。
vpn-framed-ip-netmask	特定のユーザに割り当てるネットマスクを指定します。

vpn-mode

クラスタに VPN モードを指定するには、クラスタ グループ設定モードで **vpn-mode** コマンドを使用します。vpn-mode のクラスタリング コマンドを使用すると、管理者は集中型モードと分散型モードを切り替えることができます。VPN モード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。CLI のバックアップ オプションを使用すると、管理者は VPN セッションのバックアップを別のシャーシに作成するかどうかを設定できます。このコマンドの no 形式を使用すると、設定はデフォルト値に戻ります。

vpn-mode [centralized | distributed][backup {flat | remote-chassis}]

[no] vpn-mode [centralized | distributed {flat | remote-chassis}]

デフォルト

デフォルトの VPN モードは集中型です。デフォルトのバックアップはフラットです。

構文の説明

集中型	VPN セッションは集中管理され、クラスタ マスター ユニットでのみ実行されます。
distributed	VPN セッションは、クラスタのメンバーに分散されます。
flat	バックアップ セッションは、クラスタの他のメンバーに割り当てられます。
remote-chassis	バックアップ セッションは、別のシャーシのメンバーに割り当てられます。

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	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	このコマンドが追加されました。

使用上のガイドライン

フラット バックアップ モードでは、他のクラスタ メンバーにスタンバイ セッションが確立されます。これにより、ユーザはブレード障害から保護されますが、シャーシ障害の保護は保証されません。

リモートシャーシ バックアップ モードでは、クラスタ内の別のシャーシのメンバーにスタンバイ セッションが確立されます。これにより、ユーザはブレード障害とシャーシ障害の両方から保護されます。

リモートシャーシが単一のシャーシ環境(意図的に構成されたものまたは障害の結果)で構成されている場合、別のシャーシが結合されるまでバックアップは作成されません。

例

```
ciscoasa (cfg-cluster)# vpn-mode distributed

Return the backup strategy of a distributed VPN cluster to default:
no vpn-mode distributed backup
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループの設定を行います。
show cluster vpn-sessiondb distribution	クラスタ メンバー間のアクティブ セッションとバックアップ セッションの分布を表示します。

vpnclient connect

設定済みサーバへの Easy VPN Remote 接続の確立を試行するには、グローバル コンフィギュレーション モードで **vpnclient connect** コマンドを使用します。

vpnclient connect

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

例

次に、設定済み EasyVPN サーバへの Easy VPN リモート接続の確立を試行する例を示します。

```
ciscoasa(config)# vpnclient connect
ciscoasa(config)#
```

vpnclient enable

Easy VPN Remote 機能をイネーブルにするには、グローバル コンフィギュレーション モードで **vpnclient enable** コマンドを使用します。Easy VPN Remote 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。

vpnclient enable

no vpnclient enable

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

vpnclient enable コマンドを入力すると、サポートされる ASA は Easy VPN Remote ハードウェア クライアントとして機能します。

例

次に、Easy VPN Remote 機能をイネーブルにする例を示します。

```
ciscoasa(config)# vpnclient enable
ciscoasa(config)#
```

次に、Easy VPN Remote 機能をディセーブルにする例を示します。

```
ciscoasa(config)# no vpnclient enable
ciscoasa(config)#
```

vpnclient ipsec-over-tcp

Easy VPN Remote ハードウェア クライアントとして動作している ASA を、TCP カプセル化 IPsec を使用するように設定するには、グローバル コンフィギュレーション モードで **vpnclient ipsec-over-tcp** 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。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

構文の説明

port	（任意）特定のポートを使用するように指定します。
tcp_port	（**port** キーワードを指定する場合は必須）TCP カプセル化 IPsec トンネルに使用する TCP ポート番号を指定します。

デフォルト

コマンドでポート番号を指定しない場合、Easy VPN Remote 接続では、ポート 10000 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバは、IPsec を User Datagram Protocol（UDP）パケットにカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準のカプセル化セキュリティ プロトコル（ESP、プロトコル 50）またはインターネット キー交換（IKE、UDP 500）を使用するには、TCP パケット内に IPsec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。ただし、UDP が許可されている環境では、IPsec over TCP を設定すると不要なオーバーヘッドが発生します。

TCP カプセル化 IPsec を使用するように ASA を設定する場合は、次のコマンドを入力して、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

このコマンドは、Don't Fragment（DF）ビットをカプセル化されたヘッダーからクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

例

次に、デフォルト ポート 10000 を使用して TCP カプセル化 IPsec を使用するように Easy VPN Remote ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
ciscoasa(config)# vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

次に、ポート 10501 を使用して TCP カプセル化 IPsec を使用するように Easy VPN Remote ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
ciscoasa(config)# vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

vpnclient mac-exempt

Easy VPN Remote 接続の背後にあるデバイスに対して個々のユーザ認証要件を免除するには、グローバル コンフィギュレーション モードで **vpnclient mac-exempt** 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。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

構文の説明

mac_addr_1	ドット付き 16 進表記の MAC アドレス。個々のユーザ認証を免除するデバイスの製造業者とシリアル番号を指定します。デバイスが複数の場合は、スペースで区切った各 MAC アドレスとそれぞれのネットワーク マスクを指定します。 MAC アドレスの最初の 6 文字はデバイスの製造業者を識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、ユニットの 16 進形式のシリアル番号です。
mac_mask_1	対応する MAC アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の MAC アドレスとネットワーク マスクのペアを区切ります。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

Cisco IP Phone、無線アクセス ポイント、プリンタなどのデバイスは、認証を実行できないため、個々のユニット認証がイネーブルになっている場合でも認証されません。個々のユーザ認証がイネーブルになっている場合は、このコマンドを使用してこれらのデバイスの認証を免除できます。デバイスに対する個々のユーザ認証の免除は、「デバイス パススルー」とも呼ばれます。

このコマンドでは、MAC アドレスとマスクは、3 つの 16 進数をピリオドで区切って指定します。たとえば、MAC マスク ffff.ffff.ffff は、指定した MAC アドレスとのみ一致します。すべてがゼロの MAC マスクは、いずれの MAC アドレスとも一致しません。MAC マスク ffff.ff00.0000 は、製造業者が同じであるすべてのデバイスと一致します。

（注） ヘッドエンド デバイス上で設定された個別ユーザ認証およびユーザ バイパスが必要です。たとえば、ヘッドエンド デバイスとして ASA がある場合は、グループ ポリシーに従って次のように設定します。

```
ciscoasa(config-group-policy)# user-authentication enable
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

例

Cisco IP Phone には、製造業者 ID として 00036b が設定されています。したがって、次のコマンドは、今後追加される可能性がある Cisco IP Phone も含めてすべての Cisco IP Phone を免除します。

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa(config)#
```

次に、1 つの特定の Cisco IP Phone を免除する例を示します。このようにすると、セキュリティは向上しますが、柔軟性が低くなります。

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa(config)#
```

vpnclient management

Easy VPN Remote ハードウェア クライアントへの管理アクセス用の IPsec トンネルを生成するには、グローバル コンフィギュレーション モードで **vpnclient management** コマンドを使用します。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

実行コンフィギュレーションから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、管理専用の IPsec トンネルが **split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って設定されます。

no vpnclient management

構文の説明

clear	通常のルーティングを使用して、社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセスを提供します。このオプションでは、管理トンネルは作成されません。 (注) このオプションは、クライアントとインターネット間で NAT デバイスが動作している場合に使用します。
ip_addr	Easy VPN ハードウェア クライアントからの管理トンネルを構築するホストまたはネットワークの IP アドレス。この引数は、**tunnel** キーワードとともに使用します。スペースで区切った 1 つ以上の IP アドレスとそれぞれのネットワーク マスクを指定します。
ip_mask	対応する IP アドレスのネットワーク マスク。スペースを使用して、ネットワーク マスク、および後続の IP アドレスとネットワーク マスクのペアを区切ります。
tunnel	社内ネットワークから Easy VPN クライアントとして動作している ASA 5505 の外部インターフェイスへの管理アクセス専用 IPsec トンネルを自動的に設定します。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

ASA 5505 のコンフィギュレーションに次のコマンドが含まれていることを前提とします。

- **vpnclient server**：ピアを指定します。
- **vpnclient mode**：クライアント モード（PAT）またはネットワーク拡張モードを指定します。

次のいずれかが必要です。

- **vpnclient vpngroup**：Easy VPN サーバで認証に使用するトンネル グループと IKE 事前共有キーを指定します。
- **vpnclient trustpoint**：認証に使用する RSA 証明書を識別するトラストポイントを指定します。

（注） NAT デバイスでスタティック NAT マッピングを追加しなければ、NAT デバイスの背後にある ASA のパブリック アドレスにはアクセスできません。

（注） コンフィギュレーションにかかわらず、DHCP 要求（更新メッセージを含む）は IPSec トンネル上を流れません。vpnclient management tunnel を使用しても、DHCP トラフィックは許可されません。

例

次に、ASA 5505 の外部インターフェイスから IP アドレスとマスクの組み合わせが 192.168.10.10 255.255.255.0 であるホストへの IPsec トンネルを生成する例を示します。

```
ciscoasa(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa(config)#
```

次に、IPsec を使用しないで ASA 5505 の外部インターフェイスへの管理アクセスを提供する例を示します。

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

クライアント モードまたはネットワーク拡張モードの Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient mode** 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。

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

構文の説明

client-mode	クライアント モード(PAT)を使用するように Easy VPN Remote 接続を設定します。
network-extension-mode	ネットワーク拡張モード(NEM)を使用するように Easy VPN Remote 接続を設定します。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA(リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル)にのみ適用されます。

Easy VPN クライアントは、クライアント モードまたは NEM のいずれかの動作モードをサポートします。動作モードによって、企業ネットワークからトンネル経由で内部ホスト(Easy VPN クライアントから見た場合の内部ホスト)に接続できるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

- クライアント モードでは、Easy VPN クライアントは、内部ホストからのすべての VPN トラフィックに対してポート アドレス変換(PAT)を実行します。このモードでは、ハードウェア クライアント(デフォルトの RFC 1918 アドレスが割り当てられています)の内部アドレスまたは内部ホストに対する IP アドレス管理は必要ありません。PAT により、企業ネットワークから内部ホストにはアクセスできません。

- NEM では、内部ネットワーク上のすべてのノードおよび内部インターフェイスに企業ネットワークでルーティング可能なアドレスが割り当てられます。内部ホストには、企業ネットワークからトンネル経由でアクセスできます。内部ネットワーク上のホストには、アクセス可能なサブネットから IP アドレスが（スタティックに、または DHCP によって）割り当てられます。ネットワーク拡張モードの場合、PAT は VPN トラフィックに適用されません。

（注） Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続している場合は、各ヘッドエンド デバイスで **crypto map set reverse-route** コマンドを使用して、逆ルート注入（RRI）によるリモート ネットワークのダイナミック通知を設定します。

例

次に、クライアント モードの Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# vpnclient mode client-mode
ciscoasa(config)#
```

次に、NEM の Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# vpnclient mode network-extension-mode
ciscoasa(config)#
```

vpnclient nem-st-autoconnect

NEM およびスプリット トンネリングが設定されている場合に、IPsec データ トンネルを自動的に開始するように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient nem-st-autoconnect** 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。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

vpnclient nem-st-autoconnect コマンドを入力する前に、ハードウェア クライアントのネットワーク拡張モードがイネーブルになっていることを確認します。ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPsec は、ハードウェア クライアントの背後にあるプライベート ネットワークから ASA の背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、ASA の背後にあるデバイスは、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要があります。トンネルのアップ後、いずれの側からでもデータ交換を開始できます。

(注) ネットワーク拡張モードをイネーブルするように Easy VPN サーバを設定する必要もあります。そのためには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。

ネットワーク拡張モードでは、スプリット トンネリングが設定されている場合を除き、IPsec データ トンネルが自動的に開始し、保持されます。

例

次に、スプリット トンネリングが設定されたネットワーク拡張モードで自動的に接続するように Easy VPN Remote 接続を設定する例を示します。グループ ポリシー FirstGroup のネットワーク拡張モードがイネーブルになっています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# nem enable
ciscoasa(config)# vpnclient nem-st-autoconnect
ciscoasa(config)#
```

関連コマンド

コマンド	説明
nem	ハードウェア クライアントのネットワーク拡張モードをイネーブルにします。

実行コンフィギュレーションから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。

no vpnclient sercure interface

vpnclient server

Easy VPN Remote 接続用のプライマリおよびセカンダリ IPsec サーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** 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。

vpnclient server *ip_primary_address* [*ip_secondary_address_1 ... ipsecondary_address_10*]

no vpnclient server

構文の説明

ip_primary_address	プライマリ Easy VPN（IPsec）サーバの IP アドレスまたは DNS 名。ASA または VPN 3000 コンセントレータ シリーズは、Easy VPN サーバとして機能できます。
ip_secondary_address_n	（任意）最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

接続を確立する前にサーバを設定する必要があります。**vpnclient server** コマンドでは、IPv4 アドレス、名前データベース、または DNS 名がサポートされ、アドレスはその順に解決されます。

サーバの IP アドレスまたはホスト名を使用できます。

例

次に、名前 headend-1 をアドレス 10.10.10.10 に関連付け、**vpnclient server** コマンドを使用して 3 台のサーバ（headend-dns.example.com（プライマリ）、headend-1（セカンダリ）、および 192.168.10.10（セカンダリ））を指定する例を示します。

```
ciscoasa(config)# names
ciscoasa(config)# 10.10.10.10 headend-1
ciscoasa(config)# vpnclient server headend-dns.example.com headend-1 192.168.10.10
ciscoasa(config)#
```

次に、VPN クライアントに IP アドレスが 10.10.10.15 のプライマリ IPsec サーバおよび IP アドレスが 10.10.10.30 と 192.168.10.45 のセカンダリ サーバを設定する例を示します。

```
ciscoasa(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa(config)#
```

vpnclient server-certificate

証明書マップによって指定された特定の証明書を持つ Easy VPN サーバへの接続のみを受け入れるように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient server-certificate** 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。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

構文の説明

certmap_name	受け入れ可能な Easy VPN サーバ証明書を指定する証明書マップの名前を指定します。最大長は、64 文字です。

デフォルト

Easy VPN サーバ証明書のフィルタリングは、デフォルトで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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

このコマンドを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップ自体は、crypto ca certificate map コマンドと crypto ca certificate chain コマンドを使用して定義します。

例

次に、homeservers という名前の証明書マップを持つ Easy VPN サーバへの接続のみをサポートするように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# vpnclient server-certificate homeservers
ciscoasa(config)#
```

関連コマンド

コマンド	説明
certificate	指定された証明書を追加します。
vpnclient trustpoint	Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定します。

vpnclient trustpoint

Easy VPN Remote 接続で使用する RSA アイデンティティ証明書を設定するには、グローバル コンフィギュレーション モードで **vpnclient trustpoint** 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。

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

構文の説明

chain	証明書チェーン全体を送信します。
trustpoint_name	認証に使用する RSA 証明書を識別するトラストポイン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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

crypto ca trustpoint コマンドを使用してトラストポイントを定義します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、ASA が CA 証明書を取得する方法、ASA が CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

例

次に、central という名前の特定のアイデンティティ証明書を使用し、証明書チェーン全体を送信するように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config)# vpnclient trustpoint central chain
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードを開始し、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続の VPN ユーザ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient username** 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。

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

構文の説明

xauth_password	XAUTH に使用するパスワードを指定します。最大長は、64 文字です。
xauth_username	XAUTH に使用するユーザ名を指定します。最大長は、64 文字です。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

XAUTH ユーザ名とパスワードのパラメータは、セキュア ユニット認証がディセーブルで、サーバが XAUTH クレデンシャルを要求する場合に使用します。セキュア ユニット認証がイネーブルの場合、これらのパラメータは無視され、ASA によって、ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示されます。

例

次に、XAUTH ユーザ名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する例を示します。

```
ciscoasa(config)# vpnclient username testuser password ppurkm1
ciscoasa(config)#
```

vpnclient vpngroup

Easy VPN Remote 接続の VPN トンネル グループ名とパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient vpngroup** 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。

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

構文の説明

group_name	Easy VPN サーバで設定された VPN トンネル グループの名前を指定します。最大の長さは 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバで認証に使用する IKE 事前共有キー。最大長は 128 文字です。

デフォルト

Easy VPN Remote ハードウェア クライアントとして動作している ASA の設定でトンネル グループが指定されていない場合、クライアントは RSA 証明書を使用しようとします。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Easy VPN Remote ハードウェア クライアントとして動作している ASA（リリース 7.2(1) ～ 9.2 を実行する ASA 5505、リリース 9.5(1) 以降を実行する ASA 5506 または 5508 モデル）にのみ適用されます。

事前共有キーをパスワードとして使用します。

また、接続を確立する前に、サーバを設定してモードを指定する必要もあります。

例

次に、グループ名が TestGroup1、パスワードが my_key123 の VPN トンネル グループを Easy VPN Remote 接続に設定する例を示します。

```
ciscoasa(config)# vpnclient vpngroup TestGroup1 password my_key123
ciscoasa(config)#
```

関連コマンド

コマンド	説明
vpnclient trustpoint	Easy VPN 接続で使用する RSA アイデンティティ証明書を設定します。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グローバル ポリシーまたはユーザ名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含む ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値が継承されないようにするには、**vpn-filter none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**vpn-filter** コマンドを使用して、それらの ACL を適用します。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセスリストを他のグループ ポリシーから継承しないようにします。
value *ACL name*	事前に設定済みのアクセス 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	• 対応	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	IPv4 および IPv6 ACL のサポートが追加されました。マルチ コンテキスト モードのサポートが追加されました。
9.1.(4)	IPv4 および IPv6 ACL のサポートが追加されました。廃止されたコマンド **ipv6-vpn-filter** が IPv6 ACL を指定するために誤って使用された場合、接続は終了します。

使用上のガイドライン

クライアントレス SSL VPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

設計上、vpn-filter 機能では、インバウンド方向のトラフィックだけにフィルタを適用できます。アウトバウンド ルールは自動的にコンパイルされます。icmp アクセス リストを作成するときに、方向フィルタを適用する場合は、アクセス リスト形式で icmp タイプを指定しないでください。

例

次に、FirstGroup という名前のグループ ポリシーの、acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
ipv6-vpn-filter	以前は IPv6 ACL を指定するために使用された廃止されたコマンドです。

vpn-framed-ip-address

個々のユーザに割り当てる IPv4 アドレスを指定するには、ユーザ名モードで **vpn-framed-ip-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-address {*ip_address*} {*subnet_mask*}

no vpn-framed-ip-address

構文の説明

ip_address	このユーザの IP アドレスを指定します。
subnet_mask	サブネットワーク マスクを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、anyuser という名前のユーザに IP アドレス 10.92.166.7 を設定する例を示します。

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

ユーザに専用の IPv6 アドレスを割り当てるには、ユーザ名モードで **vpn-framed-ipv6-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ipv6-address *ip_address/subnet_mask*

no vpn-framed-ipv6-address *ip_address/subnet_mask*

構文の説明

ip_address	このユーザの IP アドレスを指定します。
subnet_mask	サブネットワーク マスクを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、*anyuser* という名前のユーザに IP アドレスとネットマスク 2001::3000:1000:2000:1/64 を設定する例を示します。このアドレスは、プレフィックス値 2001:0000:0000:0000 およびインターフェイス ID 3000:1000:2000:1 を示しています。

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
ciscoasa(config-username)
```

関連コマンド

コマンド	説明
vpn-framed-ip-address	個々のユーザに割り当てる IPv4 アドレスを指定します。

vpn-group-policy

ユーザが設定済みのグループ ポリシーから属性を継承するようにするには、ユーザ名コンフィギュレーション モードで **vpn-group-policy** コマンドを使用します。グループ ポリシーをユーザ コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、ユーザはユーザ名レベルで設定されていない属性を継承できます。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

構文の説明

group-policy name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトでは、VPN ユーザにはグループ ポリシーが関連付けられません。

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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

特定ユーザのグループ ポリシーの属性値を上書きするには、その値をユーザ名モードで設定します(その属性をユーザ名モードで使用できる場合)。

例

次に、FirstGroup という名前のグループ ポリシーから属性を使用するように anyuser という名前のユーザを設定する例を示します。

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを ASA データベースに追加します。
group-policy attributes	グループ ポリシー属性モードを開始します。これにより、グループ ポリシーの AVP を設定できます。
username	ASA データベースにユーザを追加します。
username attributes	ユーザ名属性モードを開始します。これにより、特定のユーザの AVP を設定できます。

vpn-idle-timeout

ユーザ タイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。任意で、タイムアウトのアラート間隔をデフォルトの 1 分から延長できます。

実行コンフィギュレーションから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。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout {*minutes* **| none} [alert-interval** *minutes***]**

no vpn-idle-timeout

no vpn-idle-timeout alert-interval

構文の説明

分	タイムアウト期間の分数、およびタイムアウト アラートまでの分数を指定します。1 ～ 35791394 の整数を使用します。
none	AnyConnect（SSL IPsec/IKEv2）：次のコマンドで設定されたグローバル WebVPN default-idle-timeout 値（秒単位）を使用します。**ciscoasa(config-webvpn)# default-idle-timeout** WebVPN **default-idle-timeout** コマンドにおけるこの値の範囲は、60 ～ 86400 秒です。デフォルトのグローバル WebVPN アイドル タイムアウト（秒単位）は、1800 秒（30 分）です。 **（注）** すべての AnyConnect 接続では、ASA によってゼロ以外のアイドル タイムアウト値が要求されます。 WebVPN ユーザの場合、**default-idle-timeout** 値は、vpn-idle-timeout none がグループ ポリシー/ユーザ名属性に設定されている場合にのみ有効です。 サイト間（IKEv1、IKEv2）および IKEv1 リモート アクセス：タイムアウトをディセーブルにし、無制限のアイドル期間を許可します。

デフォルト

30 分。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect クライアントは、SSL および IKEv2 接続のセッション再開をサポートします。この機能により、エンドユーザ デバイスはスリープ モードに移行し、WiFi または同様の接続を失い、戻り時に同じ接続を再開できます。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-idle-timeout 30
```

セキュリティ アプライアンスは、vpn-idle-timeout 値が 0 の場合、または値が有効な範囲に該当しない場合にユーザに対して値が定義されていない場合、default-idle-timeout 値を使用します。

関連コマンド

default-idle-timeout	グローバル WebVPN デフォルト アイドル タイムアウトを指定します。
group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続の最大許容時間を設定します。この期間が終了すると、ASA は接続を終了します。

vpn load-balancing

VPN ロード バランシングおよび関連機能を設定できる VPN ロード バランシング モードを開始するには、グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを使用します。

vpn load-balancing

(注) VPN ロード バランシングを使用するには、Plus ライセンス付きの ASA 5510、または ASA 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

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	ASA 5510（Plus ライセンス付き）および 5520 以降のモデルのサポートが追加されました。

使用上のガイドライン

ロード バランシング クラスタには、セキュリティ アプライアンス モデル 5510（Plus ライセンス付き）または ASA 5520 以降を含めることができます。VPN 3000 シリーズのコンセントレータも含めることができます。混合コンフィギュレーションは可能ですが、通常は、同種クラスタにする方が容易に管理できます。

vpn load-balancing コマンドを使用して、VPN ロード バランシング モードを開始します。VPN ロード バランシング モードでは、次のコマンドを使用できます。

- **cluster encryption**
- **cluster ip address**
- **cluster key**
- **cluster port**
- **interface**
- **nat**
- **participate**
- **priority**
- **redirect-fqdn**

詳細については、個々のコマンドの説明を参照してください。

例

次に、**vpn load-balancing** コマンドの例を示します。プロンプトが変わる点に注意してください。

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

次に、interface コマンドを含む VPN load-balancing コマンド シーケンスの例を示します。interface コマンドでは、クラスタのパブリック インターフェイスを「test」、クラスタのプライベート インターフェイスを「foo」と指定しています。

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

VPN セッションまたは AnyConnect クライアント VPN セッションの最大数を指定するには、グローバル コンフィギュレーション モードで **vpn-sessiondb** コマンドを使用します。コンフィギュレーションから制限を削除するには、このコマンドの no 形式を使用します。

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number*}

構文の説明

max-anyconnect-premium-or-essentials-limit *number*	AnyConnect セッションの最大数を指定します(1 ～ライセンスで許可される最大セッションまで)。
max-other-vpn-limit *number*	AnyConnect クライアント セッション以外の VPN セッションの最大数を指定します(1 ～ライセンスで許可される最大セッションまで)。これには、Cisco VPN Client(IPsec IKEv1)および LAN-to-LAN VPN が含まれます。

デフォルト

デフォルトでは、ASA は VPN セッション数をライセンスで許可される最大数未満に制限しません。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	次のキーワードが変更されました。 • **max-anyconnect-premium-or-essentials-limit** replaced **max-session-limit** • **max-other-vpn-limit** replaced **max-webvpn-session-limit**
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、最大 AnyConnect セッションを 200 に設定する例を示します。

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	すべて、または特定のタイプの IPSec VPN セッションおよび WebVPN セッションをログオフします。
vpn-sessiondb max-webvpn-session-limit	WebVPN セッションの最大数を設定します。

vpn-sessiondb logoff

すべての VPN セッションまたは選択した VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**all** | **anyconnect** | **email-proxy** | **index** ***index_number*** | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *groupname* | **vpn-lb** | **webvpn**} [**noconfirm**]

構文の説明

all	すべての VPN セッションをログオフします。
anyconnect	すべての AnyConnect VPN クライアント セッションをログオフします。
email-proxy	(廃止)すべての電子メール プロキシ セッションをログオフします。
index *index_number*	インデックス番号で 1 つのセッションをログオフします。セッションのインデックス番号を指定します。**show vpn-sessiondb detail** コマンドを使用して、各セッションのインデックス番号を表示できます。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザ名のセッションをログオフします。

protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルは次のとおりです。 • ikev1：インターネット キー交換バージョン 1（IKEv1）プロトコルを使用するセッション。 • ikev2：インターネット キー交換バージョン 2（IKEv2）プロトコルを使用するセッション。 • ipsec：IKEv1 または IKEv2 を使用した IPsec セッション。 • ipseclan2lan：IPsec LAN-to-LAN セッション。 • ipseclan2lanovernatt：IPsec LAN-to-LAN over NAT-T セッション。 • ipsecovernatt：IPsec over NAT-T セッション。 • ipsecovertcp：IPsec over TCP セッション。 • ipsecoverudp：IPsec over UDP セッション。 • l2tpOverIpSec：L2TP over IPsec セッション。 • l2tpOverIpsecOverNatT：NAT-T を介した L2TP over IPsec セッション。 • webvpn：クライアントレス SSL VPN セッション。 • imap4s：IMAP4 セッション。 • pop3s：POP3 セッション。 • smtps：SMTP セッション。 • anyconnectParent：セッションに使用されるプロトコルに関係なく、AnyConnect クライアント セッション（AnyConnect IPsec IKEv2 セッションおよび SSL セッションを終了します）。 • ssltunnel：SSL を使用した AnyConnect セッションやクライアントレス SSL VPN セッションを含めた、SSL VPN セッション。 • dtlstunnel：DTLS がイネーブルになっている AnyConnect クライアント セッション。
ra-ikev1-ipsec	すべての IPsec IKEv1 リモート アクセス セッションをログオフします。
ra-ikev2-ipsec	すべての IPsec IKEv2 リモート アクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループ（接続プロファイル）のセッションをログオフします。
webvpn	すべてのクライアントレス SSL VPN セッションをログオフします。

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。

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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	次の **protocol** キーワードが変更または追加されました。 • **remote** が **ra-ikev1-ipsec** に変更されました。 • **ike** が **ikev1** に変更されました。 • **ikev2** が追加されました。 • **anyconnectParent** が追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.3(2)	**ra-ikev2-ipsec** キーワードが追加されました。
9.8(1)	**email-proxy** オプションが廃止されました。

例

次に、すべての AnyConnect クライアント セッションをログオフする例を示します。

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

次に、すべての IPsec セッションをログオフする例を示します。

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、ASA は接続を終了します。任意で、タイムアウトのアラート間隔をデフォルトの 1 分から延長できます。

実行コンフィギュレーションから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。このオプションを使用すると、他のグループ ポリシーからタイムアウト値を継承できます。値が継承されないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout {*minutes* | **none**} [**alert-interval** *minutes*]

no vpn-session-timeout

no vpn-session-timeout alert-interval

構文の説明

分	タイムアウト期間の分数、およびタイムアウト アラートまでの分数を指定します。1 ～ 35791394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許可します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	**alert-interval** が AnyConnect VPN に適用されました。

例

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがない場合、ASA は接続を終了します。

vpnsetup

ASA で VPN 接続を設定するための手順のリストを表示するには、グローバル コンフィギュレーション モードで **vpnsetup** コマンドを使用します。

vpnsetup {ipsec-remote-access | l2tp-remote-access | site-to-site | ssl-remote-access} steps

構文の説明

ipsec-remote-access	IPSec 接続を受け入れるように ASA を設定するための手順を表示します。
l2tp-remote-access	L2TP 接続を受け入れるように ASA を設定するための手順を表示します。
site-to-site	LAN-to-LAN 接続を受け入れるように ASA を設定するための手順を表示します。
ssl-remote-access	SSL 接続を受け入れるように ASA を設定するための手順を表示します。
steps	接続タイプの手順を表示することを指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、**vpnsetup ssl-remote-access steps** コマンドの出力例を示します。

```
ciscoasa(config-t)# vpnsetup ssl-remote-access steps

Steps to configure a remote access SSL VPN remote access connection and AnyConnect with
examples:

1. Configure and enable interface

    interface GigabitEthernet0/0
     ip address 10.10.4.200 255.255.255.0
     nameif outside
     no shutdown

    interface GigabitEthernet0/1
     ip address 192.168.0.20 255.255.255.0
```

```
     nameif inside
     no shutdown

2. Enable WebVPN on the interface

    webvpn
     enable outside

3. Configure default route

    route outside 0.0.0.0 0.0.0.0 10.10.4.200

4. Configure AAA authentication and tunnel group

    tunnel-group DefaultWEBVPNGroup type remote-access
    tunnel-group DefaultWEBVPNGroup general-attributes
     authentication-server-group LOCAL

5. If using LOCAL database, add users to the Database

    username test password t3stP@ssw0rd
    username test attributes
     service-type remote-access

Proceed to configure AnyConnect VPN client:

6. Point the ASA to an AnyConnect image

    webvpn
     svc image anyconnect-win-2.1.0148-k9.pkg

7. enable AnyConnect

    svc enable

8. Add an address pool to assign an ip address to the AnyConnect client

    ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

9. Configure group policy

    group-policy DfltGrpPolicy internal
    group-policy DfltGrpPolicy attributes
     vpn-tunnel-protocol svc webvpn

ciscoasa(config-t)#
```

関連コマンド

コマンド	説明
show running-config	ASA の実行コンフィギュレーションを表示します。

vpn-simultaneous-logins

ユーザに許可される同時ログイン数を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** 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。このオプションを使用すると、別のグループ ポリシーの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

構文の説明

整数	0 ～ 2147483647 の数字。

デフォルト

デフォルトの同時ログイン数は、3 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

(注) 同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPsec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

例

次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネル タイプ（IKEv1 または IKEv2 による IPsec、あるいは IPsec、SSL、またはクライアントレス SSL を介した L2TP）を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** 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。

vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

no vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

構文の説明

ikev1	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IKEv1 による IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
ikev2	2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IKEv2 による IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
l2tp-ipsec	L2TP 接続の IPsec トンネルをネゴシエートします。
ssl-client	SSL VPN クライアントについて SSL VPN トンネルをネゴシエートします。
ssl-clientless	HTTPS 対応の Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは必要ありません。

デフォルト

デフォルトは IPsec 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**l2tp-ipsec** キーワードが追加されました。
7.3(1)	**svc** キーワードが追加されました。
8.4(1)	**ipsec** キーワードは **ikev1** および **ikev2** キーワードに置き換えられました。

使用上のガイドライン

このコマンドを使用して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

(注) IPsec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** 引数と **ipsec** 引数の両方を設定する必要があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに対して WebVPN トンネリング モードと IPsec トンネリング モードを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn
ciscoasa(config-group-policy)# vpn-tunnel-protocol IPsec
```

関連コマンド

コマンド	説明
address pools	アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

vtep-nve

VXLAN VNI インターフェイスと VTEP 送信元インターフェイスを関連付けるには、インターフェイス コンフィギュレーション モードで **vtep-nve** コマンドを使用します。アソシエーションを削除するには、このコマンドの **no** 形式を使用します。

vtep-nve 1

no vtep-nve 1

構文の説明

1	NVE インスタンスを指定します（常に 1）。

コマンド 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。この VTEP 送信元インターフェイスを指定する NVE インスタンスを 1 つ設定できます。すべての VNI インターフェイスはこの NVE インスタンスに関連付けられている必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
```

```
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

vxlan port

VXLAN UDP ポートを設定するには、グローバル コンフィギュレーション モードで **vxlan port** コマンドを使用します。デフォルト ポートに戻すには、このコマンドの **no** 形式を使用します。

vxlan port *udp_port*

no vxlan port *udp_port*

構文の説明

udp_port	VXLAN UDP ポートを設定します。デフォルト値は 4789 です。

コマンド デフォルト

デフォルト ポートは 4789 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	トランスペアレント	シングル	コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

例

次に例を示します。

```
ciscoasa(config)# vxlan port 5678
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。

コマンド	説明
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。

CHAPTER 5

wccp コマンド～ zone-member コマンド

wccp

容量を割り当て、サービス グループに参加できるように、指定した Web Cache Communication Protocol（WCCP）サービスのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **wccp** コマンドを使用します。サービス グループをディセーブルにし、容量の割り当てを解除するには、このコマンドの no 形式を使用します。

wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]

no wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]

構文の説明

access-list	アクセス リストの名前を指定します。
group-list	（任意）サービス グループへの参加を許可する Web キャッシュを決定するアクセス リスト。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
password	（任意）サービス グループから受信したメッセージに対して Message Digest 5（MD5）認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。
password	認証で使用するパスワードを指定します。password 引数の長さは最大 7 文字です。
redirect-list	（任意）このデバイス グループにリダイレクトされたトラフィックを制御するアクセス リストとともに使用します。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。アクセス リストには、ネットワーク アドレスだけを含める必要があります。ポート固有のエントリはサポートされていません。

service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。
web-cache	Web キャッシュ サービスを指定します。 (注) Web キャッシュは、1 つのサービスとしてカウントされます。サービスの最大数（service-number 引数で割り当てられたサービスを含む）は 256 です。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、サービス グループに参加できるように WCCP をイネーブルにする例を示します。

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

wccp redirect

Web Cache Communication Protocol（WCCP）を使用したインターフェイスの入口でのパケット リダイレクションをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP リダイレ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。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

構文の説明

in	パケットがこのインターフェイスに着信するときにリダイレクションを実行するように指定します。
interface_name	パケットをリダイレクトするインターフェイスの名前。
service	サービス グループを指定します。**web-cache** キーワードを指定するか、サービスの識別番号（0 ～ 99）を指定できます。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、Web キャッシュ サービスの内部インターフェイスでの WCCP リダイレクションをイネーブルにする例を示します。

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。

web-agent-url（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

ASA が SiteMinder-type SSO 認証を要求する SSO サーバの URL を指定するには、config-webvpn-sso-siteminder モードで **web-agent-url** コマンドを使用します。

SSO サーバの認証 URL を削除するには、このコマンドの **no** 形式を使用します。

web-agent-url *url*

no web-agent-url *url*

（注） このコマンドは、SiteMinder-type SSO 認証に必要です。

構文の説明

url	SiteMinder-type SSO サーバの認証 URL を指定します。http:// または https:// を含める必要があります。

デフォルト

デフォルトでは、認証 URL は設定されません。

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	トランスペアレント	シングル	コンテキスト	システム
config-webvpn-sso-siteminder	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

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、さまざまなサーバで各種のセキュアなサービスにアクセスできます。SSO サーバには、認証要求を処理する URL があります。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

この URL に認証を送信するように ASA を設定するには、**web-agent-url** コマンドを使用します。認証 URL を設定する前に、**sso-server** コマンドを使用して SSO サーバを作成する必要があります。

セキュリティ アプライアンスと SSO サーバ間で https 通信を行うには、SSL 暗号化設定が両側で一致することを確認します。セキュリティ アプライアンスでは、これを **ssl encryption** コマンドで確認します。

例

次に、config-webvpn-sso-siteminder モードで認証 URL として http://www.example.com/webvpn を指定する例を示します。

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
ciscoasa(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	ASA 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-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
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。
ssl encryption	SSL/TLS プロトコルで使用される暗号化アルゴリズムを指定します。
sso-server	シングル サインオン サーバを作成します。

web-applications

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Application] ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **web-applications** コマンドを使用します。

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「Web Application」です。

デフォルトのタイトルのスタイルは background-color:#99CCCC;color:black;font-weight:bold;text-transform uppercase です。

デフォルトのメッセージのテキストは「Enter Web Address (URL)」です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:maroon;font-size:smaller です。

デフォルトのドロップダウンのテキストは「Web Bookmarks」です。

デフォルトのドロップダウンのスタイルは border:1px solid black;font-weight:bold;color:black;font-size:80% 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	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Applications」に変更し、テキストの色を青に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-applications title text Applications
ciscoasa(config-webvpn-custom)# web-applications title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

web-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズするには、webvpn カスタマイゼーション モードで **web-bookmarks** コマンドを使用します。

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「Web Bookmarks」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	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Web Bookmarks] のタイトルを「Corporate Web Bookmarks」にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。

webvpn（グローバル）

webvpn モードを開始するには、グローバル コンフィギュレーション モードで **webvpn** コマンドを入力します。このコマンドで入力したコマンドを削除するには、**no webvpn** コマンドを使用します。これらの **webvpn** コマンドは、すべての WebVPN ユーザに適用されます。

これらの **webvpn** コマンドを使用して、AAA サーバ、デフォルト グループ ポリシー、デフォルト アイドル タイムアウト、http プロキシと https プロキシ、WebVPN 用の NBNS サーバ、およびエンド ユーザに表示される WebVPN 画面の外観を設定できます。

webvpn

no webvpn

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

WebVPN 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	トランスペアレント	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	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

この WebVPN モードでは、WebVPN のグローバル設定を指定できます。グローバル ポリシー モードまたはユーザ名モードから WebVPN モードを開始した場合は、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。ASA クライアントレス SSL VPN 設定は、それぞれ 1 つの http-proxy コマンドと 1 つの https-proxy コマンドのみサポートしています。

（注） WebVPN が機能するためには、ブラウザ キャッシングをイネーブルにする必要があります。

例

次に、WebVPN コマンド モードを開始する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#
```

webvpn（グループポリシー属性、ユーザ名属性）

この webvpn モードを開始するには、グループポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用します。webvpn モードで入力したすべての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。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

グループ ポリシーおよびユーザ名に対する webvpn コマンドでは、ファイルへのアクセス、MAPI プロキシ、URL、および WebVPN を介した TCP アプリケーションを定義できます。ACL およびフィルタリングするトラフィックのタイプも指定します。

webvpn

no webvpn

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

WebVPN 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• 対応	—	• 対応		—
ユーザ名属性コンフィギュレーション	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル コンフィギュレーション モードから webvpn モードを開始した場合は、WebVPN のグローバル設定を指定できます。グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用すると、webvpn コマンドで指定された設定が親コマンドで指定されたグループまたはユーザに適用されます。つまり、ここで説明したグローバル ポリシー モードまたはユーザ名モードから開始した webvpn モードでは、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループ ポリシー属性モードで特定のグループ ポリシーに対して適用した WebVPN 属性は、デフォルト グループ ポリシーで指定された WebVPN 属性を上書きします。ユーザ名属性モードで特定のユーザに対して適用した WebVPN 属性は、デフォルト グループ ポリシー内およびそのユーザが属しているグループ ポリシー内の WebVPN 属性を上書きします。基本的に、これらのコマンドを使用すると、デフォルト グループまたは指定したグループ ポリシーから継承される設定を調整できます。WebVPN 設定の詳細については、グローバル コンフィギュレーション モードの **webvpn** コマンドに関する説明を参照してください。

次の表に、webvpn グループ ポリシー属性モードおよびユーザ名属性モードで設定できる属性を示します。詳細については、個々のコマンドの説明を参照してください。

属性	説明
auto-signon	WebVPN ユーザのログイン クレデンシャルを内部サーバに自動的に渡すように ASA を設定して、WebVPN ユーザにシングル サインオン方式を提供します。
customization	適用する設定済み WebVPN カスタマイゼーションを指定します。
deny-message	アクセスが拒否されたときにユーザに表示されるメッセージを指定します。
filter	WebVPN 接続に使用するアクセス リストを指定します。
functions	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を介した URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示される Web ページの URL を設定します。
html-content-filter	WebVPN セッションでフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
http-comp	使用する HTTP 圧縮アルゴリズムを指定します。
keep-alive-ignore	セッションの更新で無視する最大オブジェクト サイズを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに対する TCP ポート フォワーディングを識別する表示名を設定します。
sso-server	SSO サーバ名を設定します。
svc	SSL VPN クライアント属性を設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバと URL のリストを指定します。

例

次に、「FirstGroup」という名前のグループ ポリシーの webvpn モードを開始する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-webvpn)#
```

次に、「test」というユーザ名の webvpn モードを開始する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-webvpn)#
```

関連コマンド

clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

whitelist

クラウド Web セキュリティのために、トラフィックのクラスでホワイトリスト アクションを実行するには、クラス コンフィギュレーション モードで **whitelist** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect scansafe** コマンドを入力し、次に **parameters** コマンドを入力します。ホワイトリス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。

whitelist

no whitelist

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。

コマンド 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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

class-map type inspect scansafe コマンドを使用して、ホワイトリストに記載するトラフィックを識別します。**policy-map type inspect scansafe** コマンドでインスペクション クラス マップを使用し、クラスのホワイトリスト アクションを指定します。**inspect scansafe** コマンドでインスペクション ポリシー マップを呼び出します。

例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザおよびグループをホワイトリストに記載する例を示します。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
```

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {primary | backup}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。

who

ASA 上のアクティブな Telnet 管理セッションを表示するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

構文の説明

local_ip	（任意）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限することを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

who コマンドを使用すると、現在 ASA にログインしている各 Telnet クライアントの TTY_ID と IP アドレスを表示できます。

例

次に、クライアントが Telnet セッションを使用して ASA にログインしている場合の **who** コマンドの出力例を示します。

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	ASA コンソールへの Telnet アクセスを追加して、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** 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。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

構文の説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続の許可です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用して、ウィンドウ サイズが縮小されたすべての接続をドロップします。

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

例

次に、さまざまなウィンドウ サイズの接続をすべてドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# window-variation drop-connection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **wins-server** 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。このオプションを使用すると、他のグループ ポリシーから WINS サーバを継承できます。サーバが継承されないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

構文の説明

none	WINS サーバをヌル値に設定して、WINS サーバを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。複数のサーバを設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーに IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の WINS サーバを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

without-csd

特定のユーザがグループ URL テーブル内のいずれかのエントリを入力して VPN セッションを確立する場合に、そのユーザに対して接続ごとのプロファイルに基づく Cisco Secure Desktop の Hostscan アプリケーションの実行を免除するには、トンネル webvpn コンフィギュレーション モードで **without-csd** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

without-csd [**anyconnect**]

no without-csd [**anyconnect**]

構文の説明

anyconnect	（オプション）AnyConnect 接続だけに影響するようにコマンドを変更します。

デフォルト

デフォルト値はありません。インストールしている場合、Hostscan 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	トランスペアレント	シングル	コンテキスト	システム
トンネル webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.2(1)	**anyconnect** 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、ユーザがこの接続プロファイル（CLI ではトンネル グループと呼ばれます）に設定された URL グループ リスト内の URL を入力した場合に、Cisco Secure Desktop の Hostscan アプリケーションがエンドポイントで実行されません。このコマンドを入力すると、これらのセッションのエンドポイント状態が検出されないため、ダイナミック アクセス ポリシー（DAP）コンフィギュレーションを調整する必要があります。

例

次の例では、最初のコマンドでグループ URL を作成しています。「example.com」が ASA のドメイン、「no-csd」が URL の一意の部分です。ユーザがこの URL を入力すると、ASA は、この接続プロファイルをセッションに割り当てます。**group-url** コマンドは、**without-csd** コマンドを有効にするために必要です。**without-csd** コマンドは、ユーザに対して Cisco Secure Desktop の実行を免除します。

```
ciscoasa(config-tunnel-webvpn)# group-url https://example.com/no-csd enable
ciscoasa(config-tunnel-webvpn)# without-csd
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
csd enable	without-csd コマンドが含まれていないすべての接続プロファイルに対して Cisco Secure Desktop をイネーブルにします。
csd image	コマンドで指定された Cisco Secure Desktop イメージを、パスで指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。
group-url	この接続プロファイルに固有のグループ URL を作成します。

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定します。コンテキスト コンフィギュレーションを削除する場合は、ファイルをリモート サーバ（指定されている場合）から手動で削除するか、またはシステム実行スペースで **delete** コマンドを使用してファイルをフラッシュ メモリからクリアできます。

ASAv の場合、このコマンドは**リロード**後に導入設定（初期の仮想導入設定）を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。導入設定を消去し、ASA アプライアンスの場合と同じ工場出荷時のデフォルト設定を適用するには、**configure factory-default** を参照してください。

（注） ASAv は現在実行されているイメージをブートするため、元のブート イメージには戻りません。

リロード前にコンフィギュレーションを保存しないでください。

フェールオーバー ペアの ASAv の場合は、最初にスタンバイ ユニットの電源をオフにします。スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブ ユニットから同期し、必要な導入コンフィギュレーションが消去されます。アクティブ ユニットのリロード後、スタンバイ ユニットの電源をオンにすることができます。その後、導入コンフィギュレーションはスタンバイ ユニットに同期します。

例

次に、スタートアップ コンフィギュレーションを消去する例を示します。

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write memory

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory [**all** [**/noconfirm**]]

構文の説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトを表示しません。
all	マルチ コンテキスト モードのシステム実行スペースでこのキーワードを使用すると、すべてのコンテキスト コンフィギュレーションおよびシステム コンフィギュレーションが保存されます。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	**all** キーワードを使用して、すべてのコンテキスト コンフィギュレーションを保存できるようになりました。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。変更内容は、起動時に実行メモリにロードされるスタートアップ コンフィギュレーションに保存した場合、次のリブートまでの間のみ保持されます。シングル コンテキスト モードまたはマルチ コンテキスト モードにおけるシステムのスタートアップ コンフィギュレーションの場所は、**boot config** コマンドを使用して、デフォルトの場所（隠しファイル）から選択した場所に変更できます。マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定された場所にあります。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力して、現在のコンテキスト コンフィギュレーションを保存できます。すべてのコンテキスト コンフィギュレーションを保存するには、システム実行スペースで **write memory all** コマンドを入力します。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、ASA は、コンフィギュレーションをサーバに戻して保存できない HTTP および HTTPS の URL を除き、**config-url** コマンドで指定されたサーバにコンフィギュレーションを戻して保存します。ASA が **write memory all** コマンドを使用して各コンテキストを保存した後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context 'a' , context 'x' , context 'z' .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- フラッシュ メモリに不良セクターがあるためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

システムでは、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるため、**write memory** コマンドでも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次に、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する例を示します。

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

実行コンフィギュレーションを TFTP サーバに保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 ファイル名をこのコマンドと **tftp-server** コマンドで指定した場合、ASA は **tftp-server** コマンドのファイル名をディレクトリとして処理し、**write net** コマンドのファイル名をそのディレクトリの下にファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ(//)が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバでこのタイプの URL がサポートされていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン(:)の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。 デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。

マルチ コンテキスト モードの場合、このコマンドは現在のコンフィギュレーションを保存します。1 つのコマンドですべてのコンテキストを保存することはできません。このコマンドを、システムおよび各コンテキストに対して個別に入力する必要があります。**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、**write memory** コマンドでは、管理コンテキスト インターフェイスを使用してスタートアップ コンフィギュレーションに保存します。これは、システムで、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるからです。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次に、**tftp-server** コマンドで TFTP サーバおよびファイル名を設定する例を示します。

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドは入力されていません。

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドでディレクトリ名が設定され、サーバ アドレスは上書きされます。

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置に ASA またはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションのスタンバイ ユニットまたはスタンバイ フェールオーバー グループと、アクティブなユニットまたはフェールオーバー グループのコンフィギュレーションとの同期が失われた場合にのみ、使用します。通常、この状態は、コマンドがスタンバイ ユニットまたはスタンバイ フェールオーバー グループで直接入力された場合に発生します。

アクティブ/スタンバイ フェールオーバーの場合、アクティブ ユニットで入力された **write standby** コマンドは、スタンバイ ユニットの実行コンフィギュレーションにアクティブ フェールオーバー ユニットの実行コンフィギュレーションを書き込みます。

アクティブ/アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力した場合は、ASA 上のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストのコンフィギュレーションがピア ユニットに書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。
- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

write standby コマンドは、コンフィギュレーションをピア ユニットの実行コンフィギュレーションに複製します。コンフィギュレーションは、スタートアップ コンフィギュレーションに保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したユニットで **copy running-config startup-config** コマンドを使用します。コマンドはピア ユニットに複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

ステートフル フェールオーバーがイネーブルの場合、**write standby** コマンドは、コンフィギュレーションのレプリケーションが完了した後、状態情報もスタンバイ ユニットに複製します。マルチ コンテキスト モードでは、ステート情報を複製するには、コンテキスト内で **write standby** を入力して状態情報を複製します。

(注) **write standby** コマンドを入力した後、設定が再同期されるまでの間、フェールオーバー インターフェイスが一時的に停止します。また、これにより、フェールオーバー状態のインターフェイスの検出に一時的な障害が発生します。

例

次に、現在の実行コンフィギュレーションをスタンバイ ユニットに書き込む例を示します。

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ ユニットを強制的にリブートします。

write terminal

端末で実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次に、実行コンフィギュレーションを端末に書き込む例を示します。

```
ciscoasa# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

xlate block-allocation

キャリアグレードまたは大規模な PAT 向けにポート ブロック割り当ての特性を設定するには、グローバル コンフィギュレーション モードで **xlate block-allocation** 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。

xlate block-allocation {**size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds*}

no xlate block-allocation {**size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds*}

構文の説明

size *value*	ブロック割り当てサイズ。これは、各ブロックのポート数です。 範囲は 32 ～ 4096 です。デフォルトは 512 です。 デフォルトを使用しない場合は、選択したサイズが 64,512 に均等に分割していることを確認します（1024 ～ 65535 の範囲のポート数）。そうしなければ、割り当てることができないポートが発生します。たとえば、100 を指定すると 12 個の未使用ポートが生じます。
maximum-per-host *number*	ホスト 1 つあたりに割り当てることができる最大ブロック。制限はプロトコルごとに設定されるので、制限「4」は、ホストごとの上限が 4 つの UDP ブロック、4 つの TCP ブロック、および 4 つの ICMP ブロックであることを意味します。 指定できる値の範囲は 1 ～ 8 で、デフォルトは 4 です。
pba-interim-logging *seconds*	暫定ロギングを有効にします。デフォルトでは、ポート ブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ログの記録を有効にすると、指定した間隔でメッセージ 305017 が生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。間隔は 21600 ～ 604800 秒（6 時間から 7 日間）を指定することができます。

コマンド デフォルト

デフォルトの割り当てサイズは 512 です。ホスト 1 つあたりのデフォルトの上限値は 4 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。
9.12(1)	**pba-interim-logging** コマンドが追加されました。

使用上のガイドライン

キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ブロックのポートを使用する最後の xlate が削除されると、ブロックが解放されます。

ポート ブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。そのため、小さいポート番号（1 ～ 1023）がアプリケーションに必要な場合、これは機能しません。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内およびホストに割り当てられたブロック内でマップされるポートを取得します。

xlate block-allocation コマンドは、これらのポート ブロックの特性を設定します。PAT プールの使用時に PAT ルールに従って ポート ブロック割り当てを有効にするには、**nat** コマンドで block-allocation キーワードを使用します。

例

次に、ポート ブロック割り当て特性の変更例と、オブジェクト NAT ルールで PAT プール用にポート ブロック割り当てを実装する例を示します。

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6
xlate block-allocation pba-interim-logging 21600

object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat dynamic pat-pool mapped-pat-pool block-allocation
```

関連コマンド

コマンド	説明
nat（グローバル）	Twice NAT ルールを追加します。
nat（オブジェクト）	オブジェクト NAT ルールを追加します。
show local-host	ホストに割り当てられたポート ブロックを示します。
show running-config xlate	**xlate** 設定を示します。

xlate per-session

Multi-Session PAT を使用するには、グローバル コンフィギュレーション モードで **xlate per-session** コマンドを使用します。Multi-Session PAT ルールを削除するには、このコマンドの **no** 形式を使用します。

xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

no xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

構文の説明

deny	拒否ルールを作成します。
destination_ip	宛先 IP アドレスについて、次のように設定できます。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。
operator dest_port	*operator* は、宛先で使用されるポート番号に一致します。使用できる演算子は、次のとおりです。 • lt：より小さい • gt：より大きい • eq：等しい • neq：等しくない • range：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
operator ***src_port***	（オプション）*operator* は、ソースで使用されるポート番号に一致します。使用できる演算子は、次のとおりです。 • lt：より小さい • gt：より大きい • eq：等しい • neq：等しくない • range：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
permit	許可ルールを作成します。

source_ip	送信元 IP アドレスについて、次のように設定できます。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	UDP トラフィックを指定します。

コマンド デフォルト

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。次のデフォルト ルールがインストールされています。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

(注) これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次の拒否ルールを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Per-session PAT 機能によって PAT の拡張性が向上し、クラスタリングの場合に各メンバー ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/*平均ライフタイム*です。

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。H.323、SIP、Skinny など、Multi-Session PAT による利点があるトラフィックの場合、Per-Session PAT 拒否ルールを作成して、Per-Session PAT をディセーブルにできます。

Per-Session PAT ルールを追加する場合、ルールはデフォルト ルールの上位に配置されますが、他の手動で作成されたルールの下位に配置されます。ルールは必ず、適用する順序で作成してください。

例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
ciscoasa(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
ciscoasa(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

関連コマンド

コマンド	説明
clear configure xlate	**xlate per-session** ルールをクリアします。
nat（グローバル）	Twice NAT ルールを追加します。
nat（オブジェクト）	オブジェクト NAT ルールを追加します。
show running-config xlate	**xlate per-session** ルールを表示します。

zone

トラフィック ゾーンを追加するには、グローバル コンフィギュレーション モードで **zone** コマンドを使用します。ゾーンを削除するには、このコマンドの **no** 形式を使用します。

zone *name*

no zone *name*

構文の説明

name	最大 48 文字でゾーン名を設定します。

コマンド 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		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

1 つの *トラフィック ゾーン*に複数のインターフェイスを割り当てることができます。これにより、ゾーン内の任意のインターフェイスで、既存のフローのトラフィックが ASA に出入りできるようになります。この機能により、ASA 上での Equal-Cost Multi-Path（ECMP）ルーティング、および ASA へのトラフィックの複数のインターフェイスにわたる外部ロード バランシングが可能になります。

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。

最大 256 ゾーンを作成できます。

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

関連コマンド

コマンド	説明
clear configure zone	ゾーンのコンフィギュレーションをクリアします。
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
show asp table routing	デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。
show asp table zone	デバッグ目的で高速セキュリティ パス テーブルを表示します。
show conn long	ゾーンの接続情報を表示します。
show local-host zone	ゾーン内のローカル ホストのネットワーク状態を表示します。
show nameif zone	インターフェイス名およびゾーン名を表示します。
show route zone	ゾーン インターフェイスのルートを表示します。
show running-config zone	ゾーンのコンフィギュレーションを表示します。
show zone	ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。
zone-member	トラフィック ゾーンにインターフェイスを割り当てます。

zonelabs-integrity fail-close

ASA と Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生したときに VPN クライアントへの接続が閉じるように ASA 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 **zonelabs-integrity fail-close** コマンドを使用します。Zone Labs 接続で障害が発生しても VPN 接続を開いたままにする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。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

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

デフォルトでは、接続は障害が発生しても開いたままです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバが ASA に応答しない場合も、ASA はプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。

Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても ASA によってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバが応答しない場合、または接続が中断された場合に、VPN クライアント接続を閉じるように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、ASA への VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバを ASA が到達不能と見なすまでの秒数を指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。

zonelabs-integrity fail-open

ASA と Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生した後も、ASA へのリモート VPN クライアント接続を開いたままにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-open** コマンドを使用します。Zone Labs サーバ接続で障害が発生した場合に VPN クライアントへの接続を閉じるには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

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

デフォルトでは、ASA で Zone Labs Integrity ファイアウォール サーバへの接続が確立または維持されない場合、リモート VPN 接続は開いたままになります。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバが ASA に応答しない場合も、ASA はプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても ASA によってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドまたは **no zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても VPN クライアント接続を開いたままにするデフォルト状態に戻す例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバを ASA が到達不能と見なすまでの秒数を指定します。

zonelabs-integrity fail-timeout

ASA において、何秒経過すると応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすかを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-timeout** コマンドを使用します。デフォルトのタイムアウト（10 秒）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

構文の説明

timeout	ASA において、応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすまでの秒数。設定可能な値の範囲は、5 ～ 20 秒です。

デフォルト

デフォルトのタイムアウト値は 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が指定された秒数待機しても Zone Labs サーバから応答がない場合、サーバは応答不能と見なされます。VPN クライアントへの接続は、デフォルトまたは **zonelabs-integrity fail-open** コマンドの設定に従って開いたままになります。ただし、**zonelabs-integrity fail-close** コマンドが発行されている場合は、ASA で Integrity サーバが応答不能と見なされると接続は閉じます。

例

次に、12 秒経過後にアクティブな Zone Labs Integrity サーバを到達不能と見なすように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、ASA への VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。

zonelabs-integrity interface

Zone Labs Integrity サーバとの通信で使用する ASA インターフェイスを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity interface** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのインターフェイスをデフォルト（none）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。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

構文の説明

interface	Zone Labs Integrity ファイアウォール サーバが通信する ASA インターフェイスを指定します。これは、多くの場合、**nameif** コマンドで作成されたインターフェイス名です。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール インターフェイスは none に設定されます。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、IP アドレス範囲 10.0.0.5 ～ 10.0.0.7 を使用して 3 台の Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、ポート 300 および inside というインターフェイスでサーバをリッスンするように ASA を設定しています。

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)# zonelabs-integrity interface inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity port

Zone Labs Integrity ファイアウォール サーバとの通信で使用する ASA 上のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity port** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのデフォルト ポート 5054 に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

構文の説明

port	ASA 上の Zone Labs Integrity ファイアウォール サーバのポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバのポートの番号。指定できる範囲は、10 ～ 10000 です。

デフォルト

Zone Labs Integrity ファイアウォール サーバのデフォルト ポートは 5054 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、**zonelabs-integrity port** コマンドと **zonelabs-integrity interface** コマンドでそれぞれ設定されたポートとインターフェイスで Zone Labs Integrity ファイアウォール サーバをリッスンします。

(注) ユーザ インターフェイスが最大 5 つの Integrity サーバのコンフィギュレーションをサポートしている場合でも、現在のリリースの ASA が一度にサポートする Integrity サーバは 1 つです。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 を使用して Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、デフォルト ポート 5054 ではなくポート 300 でアクティブな Zone Labs サーバをリッスンするように ASA を設定しています。

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity server-address

Zone Labs Integrity ファイアウォール サーバを ASA コンフィギュレーションに追加するには、グローバル コンフィギュレーション モードで **zonelabs-integrity server-address** コマンドを使用します。Zone Labs サーバを IP アドレスまたはホスト名で指定します。

Zone Labs Integrity ファイアウォール サーバを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

(注) ユーザ インターフェイスは複数の Integrity サーバのコンフィギュレーションをサポートしているように見えますが、現在のリリースの ASA では同時に 1 台のサーバのみがサポートされます。

構文の説明

hostname	Zone Labs Integrity ファイアウォール サーバのホスト名を指定します。ホスト名のガイドラインについては、**name** コマンドを参照してください。
ip-address	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

コマンド デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは設定されません。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このリリースでは、1 台の Zone Labs Integrity ファイアウォール サーバを設定できます。そのサーバで障害が発生した場合は、まず別の Integrity サーバを設定してからクライアント VPN セッションを再確立します。

サーバをホスト名で指定するには、まず **name** コマンドを使用して Zone Labs サーバ名を設定する必要があります。**name** コマンドを使用する前に、**names** コマンドを使用してコマンドをイネーブルにします。

(注) 現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 にサーバ名 ZL-Integrity-Svr を割り当て、その名前を使用して Zone Labs Integrity サーバを設定する例を示します。

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-certificate-port

SSL 証明書を取得する場合に Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-certificate-port** コマンドを使用します。デフォルト ポート番号（80）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

構文の説明

cert-port-number	SSL 証明書を要求する場合に Zone Labs Integrity ファイアウォール サーバが接続する ASA のポート番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは SSL 証明書を ASA のポート 80 で要求します。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA と Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、ASA が SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（ASA）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。**zonelabs-integrity ssl-certificate-port** コマンドで、Zone Labs サーバが SSL サーバ証明書を要求する場合に接続するポートを指定します。

例

次に、ASA のポート 30 で Zone Labs Integrity サーバから SSL 証明書要求を受信するように設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-client-authentication

Zone Labs Integrity ファイアウォール サーバの SSL 証明書を ASA で認証できるようにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-client-authentication** コマンドを *enable* 引数を指定して使用します。Zone Labs の SSL 証明書の認証をディセーブルにするには、*disable* 引数を使用するか、またはこのコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

構文の説明

disable	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。
enable	ASA で Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証することを指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバの SSL 証明書の ASA による認証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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA と Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、ASA が SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（ASA）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。ただし、クライアント証明書の認証は任意です。Zone Labs サーバの（SSL クライアント）証明書の ASA による認証をイネーブルまたはディセーブルにするには、**zonelabs-integrity ssl-client-authentication** コマンドを使用します。

例

次に、Zone Labs Integrity サーバの SSL 証明書を認証するように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。

zone-member

トラフィック ゾーンにインターフェイス追加するには、インターフェイス コンフィギュレーション モードで **zone-member** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

zone-member *name*

no zone-member *name*

構文の説明

name	**zone** コマンドで設定されたゾーン名を指定します。

コマンド 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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

名前、IP アドレス、およびセキュリティ レベルを含むすべてのインターフェイス パラメータを設定します。ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

次のタイプのインターフェイスをゾーンに追加できます。

- 物理
- VLAN
- EtherChannel
- 冗長

次のタイプのインターフェイスは追加できません。

- 管理専用
- 管理アクセス
- フェールオーバーまたはステート リンク
- クラスタ制御リンク
- EtherChannel インターフェイスまたは冗長インターフェイスのメンバー インターフェイス

1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。

ゾーンごとに最大 8 つのインターフェイスを含めることができます。

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

関連コマンド

コマンド	説明
clear configure zone	ゾーンのコンフィギュレーションをクリアします。
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
show asp table routing	デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。
show asp table zone	デバッグ目的で高速セキュリティ パス テーブルを表示します。
show conn long	ゾーンの接続情報を表示します。
show local-host zone	ゾーン内のローカル ホストのネットワーク状態を表示します。
show nameif zone	インターフェイス名およびゾーン名を表示します。
show route zone	ゾーン インターフェイスのルートを表示します。
show running-config zone	ゾーンのコンフィギュレーションを表示します。
show zone	ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。
zone	トラフィック ゾーンを設定します。

パート 2

ASA サービス モジュール用 Cisco IOS コマンド

CHAPTER 6

ASASM 用 Cisco IOS コマンド

clear diagnostics loopback

オンライン診断テストの設定をクリアするには、特権 EXEC モードで **clear diagnostic loopback** コマンドを使用します。

clear diagnostics loopback

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

特権 EXEC

使用上のガイドライン

clear diagnostics loopback コマンドはオンライン診断テストの設定をクリアします。

例

次に、**clear diagnostics loopback** コマンドの出力例を示します。

```
ciscoasa# clear diagnostics loopback

Port    Test    Pkts-received  Failures
0       0       0              0
1       0       0              0
```

関連コマンド

コマンド	説明
show diagnostics loopback	PC のループバック テストに関連する情報、テスト実行数、受信したループバック パケット数、および検出された障害数を表示します。

firewall autostate

自動ステート メッセージングをイネーブルにするには、グローバル コンフィギュレーション モードで **firewall autostate** コマンドを使用します。自動ステート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。

firewall autostate

no firewall autostate

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

デフォルトでは、自動ステートはディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

使用上のガイドライン

自動ステート メッセージングを行うと、スイッチ インターフェイスに障害が発生したか、起動したかについて、ASA ですばやく検出できます。スーパーバイザ エンジンから ASA に、ASA VLAN に関連付けられている物理インターフェイスのステータスに関する自動ステート メッセージが送信されます。たとえば、VLAN に関連付けられたすべての物理インターフェイスが停止すると、VLAN が停止したことを示す自動ステート メッセージが ASA に届きます。この情報に基づいて ASA は VLAN が停止していると判断できます。この場合は、いずれの側でリンク障害が発生したかを判別するのに必要となるインターフェイス モニタリング テストが回避されます。自動ステート メッセージングにより、ASA がリンク障害を検出するのに要する時間が大幅に短縮されます（自動ステートがサポートされていない場合の最長 45 秒と比較すると、数ミリ秒も短縮されます）。

次の場合に、スイッチのスーパーバイザから ASA に自動ステート メッセージが送信されます。

- VLAN に属している最後のインターフェイスが停止した
- VLAN に属している最初のインターフェイスが動作を開始した

例

次の例では、自動ステート メッセージングをイネーブルにします。

```
Router(config)# firewall autostate
```

関連コマンド

コマンド	説明
show firewall autostate	自動ステート機能の設定内容を表示します。

firewall module

ファイアウォール グループを ASA に割り当てるには、グローバル コンフィギュレーション モードで **firewall module** コマンドを入力します。このグループを削除するには、このコマンドの **no** 形式を使用します。

firewall module *module_number* **vlan-group** *firewall_group*

no firewall module *module_number* **vlan-group** *firewall_group*

構文の説明

module_number	モジュール番号を指定します。インストールされたモジュールとその番号を表示するには、**show module** コマンドを使用します。
vlan-group *firewall_group*	**firewall vlan-group** コマンドで定義されている 1 つ以上のグループ番号を指定します。 • 個別の番号（*n*） • 範囲（*n-x*） 番号または範囲はカンマで区切ります。番号の入力例を示します。 `5,7-10`

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

グローバル コンフィギュレーション

使用上のガイドライン

- ASASM ごとに最大 16 個のファイアウォール VLAN グループを割り当てることができます。（Cisco IOS ソフトウェアで 16 より多くの VLAN グループを作成できますが、各 ASASM に割り当てることができるのは 16 グループのみです）。グループを作成するには、**firewall vlan-group** コマンドを参照してください。たとえば、すべての VLAN を 1 つのグループに割り当てる、内部グループと外部グループを作成する、またはカスタマーごとにグループを 1 つずつ作成するといったことが可能です。
- グループごとの VLAN の数に制限はありませんが、ASASM は VLAN を ASASM システム制限までしか使用できません（詳細については、ASASM ライセンス マニュアルを参照してください）。
- 同じ VLAN を複数のファイアウォール グループに関連付けることはできません。
- 複数の ASASM に 1 つのファイアウォール グループを割り当てることができます。たとえば、複数の ASASM に割り当てる VLAN は、それぞれの ASASM に一意の VLAN とは別のグループに配置できます。
- 同一スイッチ シャーシ内で ASASM フェールオーバーを使用する場合は、フェールオーバーおよびステートフル通信のために確保してある VLAN（複数可）をスイッチ ポートに割り当てないでください。ただし、シャーシ間でフェールオーバーを使用する場合は、シャーシ間を結ぶトランク ポートに VLAN を組み込む必要があります。

- ASASM に VLAN を割り当てる前に、スイッチに VLAN を追加しなかった場合、VLAN はスーパーバイザ エンジンのデータベースに保管され、スイッチに追加された時点で ASASM に送信されます。
- VLAN がスイッチに割り当てられる前に、ASASM コンフィギュレーションに VLAN を設定できます。スイッチが VLAN を ASASM に送信すると、ASASM コンフィギュレーションでシャットダウンするかどうかにかかわらず、VLAN は ASASM 上で、デフォルトで管理上アップ状態になることに注意してください。この場合、再度シャットダウンする必要があります。

例

次の例では、3 つのファイアウォール VLAN グループ（各 ASA に 1 グループずつ、および両方の ASA に割り当てられた VLAN を含む 1 グループ）を作成する方法を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

次に、**show firewall vlan-group** コマンドの出力例を示します。

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

次に、すべての VLAN グループを示す **show firewall module** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

関連コマンド

コマンド	説明
firewall vlan-group	VLAN を VLAN グループに割り当てます。
show firewall module vlan-group	VLAN グループと、これに割り当てられた VLAN を表示します。
show module	インストールされているすべてのモジュールを表示します。

firewall multiple-vlan-interfaces

複数の SVI を ASA に追加できるようにするには、グローバル コンフィギュレーション モードで **firewall multiple-vlan-interfaces** 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。

firewall multiple-vlan-interfaces

no firewall multiple-vlan-interfaces

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

デフォルトでは、複数の SVI は許可されません。

コマンド モード

グローバル コンフィギュレーション

使用上のガイドライン

MSFC 上で定義された VLAN をスイッチ仮想インターフェイス（SVI）といいます。SVI 用の VLAN を ASA に割り当てると、MSFC は、ASA と他のレイヤ 3 VLAN 間でルーティングを行います。セキュリティ上の理由から、デフォルトでは MSFC と ASA 間に配置できる SVI は 1 つだけです。たとえば、誤って複数の SVI をシステムに設定した場合は、MSFC に内部 VLAN と外部 VLAN の両方が割り当てられていることによって、トラフィックが偶発的に ASA をバイパスする可能性があります。

ただし、ネットワーク シナリオの中には、ASA をバイパスする必要があるものもあります。たとえば、IP ホストと同じイーサネット セグメント上に IPX ホストが配置されている場合、複数の SVI を使用する必要があります。ルーテッド ファイアウォール モードの ASA は IP トラフィックしか処理せず、IPX などの他のプロトコル トラフィックを廃棄するため（トランスペアレント ファイアウォール モードでは、IP 以外のトラフィックを許可することもできます）、IPX トラフィックで ASA をバイパスする必要があります。この場合、必ず、VLAN を通過できるのが IPX トラフィックに限定されるアクセス リストを使用して MSFC を設定してください。

トランスペアレント ファイアウォールがマルチ コンテキスト モードの場合、コンテキストごとに対応する外部インターフェイス上に固有の VLAN が必要なため、複数の SVI を使用する必要があります。ルーテッド モードの場合でも複数の SVI を使用できるので、外部インターフェイス用に 1 つの VLAN を共有する必要はありません。

例

次に、複数の SVI を使用する一般的な設定例を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

次に、**show interface** コマンドの出力例を示します。

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN グループを定義します。

firewall vlan-group

VLAN をファイアウォール グループに割り当てるには、グローバル コンフィギュレーション モードで **firewall vlan-group** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

no firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

構文の説明

firewall_group	整数のグループ ID を指定します。
vlan_range	グループに割り当てる VLAN を指定します。*vlan_range* 値には、次のいずれかの形式で 1 つまたは複数の VLAN（2 ～ 1000 および 1025 ～ 4094）を指定できます。 • 個別の番号（*n*） • 範囲（*n-x*） 番号または範囲はカンマで区切ります。番号の入力例を示します。 `5,7-10,13,45-100` **（注）** ルーテッド ポートと WAN ポートは内部 VLAN を使用するため、1020 ～ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。
switch {**1** | **2**}	（オプション）VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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

グローバル コンフィギュレーション

使用上のガイドライン

- **firewall module** コマンドを使用して、ASASM ごとに最大 16 個のファイアウォール VLAN グループを割り当てることができます。（Cisco IOS ソフトウェアで 16 より多くの VLAN グループを作成できますが、各 ASASM に割り当てることができるのは 16 グループのみです）。たとえば、すべての VLAN を 1 つのグループに割り当てる、内部グループと外部グループを作成する、またはカスタマーごとにグループを 1 つずつ作成するといったことが可能です。
- グループごとの VLAN の数に制限はありませんが、ASASM は VLAN を ASASM システム制限までしか使用できません（詳細については、ASASM ライセンス マニュアルを参照してください）。
- 同じ VLAN を複数のファイアウォール グループに関連付けることはできません。
- 複数の ASASM に 1 つのファイアウォール グループを割り当てることができます。たとえば、複数の ASASM に割り当てる VLAN は、それぞれの ASASM に一意の VLAN とは別のグループに配置できます。
- VLAN ID 2 ～ 1000 および 1025 ～ 4094 を使用します。

- ルーテッド ポートと WAN ポートは内部 VLAN を使用するため、1020 ～ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。
- 予約済みの VLAN は使用できません。
- VLAN 1 は使用できません。
- 同一スイッチ シャーシ内で ASASM フェールオーバーを使用する場合は、フェールオーバーおよびステートフル通信のために確保してある VLAN（複数可）をスイッチ ポートに割り当てないでください。ただし、シャーシ間でフェールオーバーを使用する場合は、シャーシ間を結ぶトランク ポートに VLAN を組み込む必要があります。
- ASASM に VLAN を割り当てる前に、スイッチに VLAN を追加しなかった場合、VLAN はスーパーバイザ エンジンのデータベースに保管され、スイッチに追加された時点で ASASM に送信されます。
- VLAN がスイッチに割り当てられる前に、ASASM コンフィギュレーションに VLAN を設定できます。スイッチが VLAN を ASASM に送信すると、ASASM コンフィギュレーションでシャットダウンするかどうかにかかわらず、VLAN は ASASM 上で、デフォルトで管理上アップ状態になることに注意してください。この場合、再度シャットダウンする必要があります。

例

次の例では、3 つのファイアウォール VLAN グループ（各 ASA に 1 グループずつ、および両方の ASA に割り当てられた VLAN を含む 1 グループ）を作成する方法を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

次に、**show firewall vlan-group** コマンドの出力例を示します。

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

次に、すべての VLAN グループを示す **show firewall module** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
show firewall vlan-group	VLAN グループと、これに割り当てられた VLAN を表示します。
show module	インストールされているすべてのモジュールを表示します。

service-module session

スイッチの CLI から ASASM にコンソール アクセスするには、特権 EXEC モードで **service-module session** コマンドを入力します。

service-module session [**switch** {**1** | **2**}] **slot** *number*

構文の説明

slot *number*	ASASM のスロット番号を指定します。モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。
switch {**1**	**2**}	（オプション）VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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

特権 EXEC

使用上のガイドライン

service-module session コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続は、実際のコンソール接続の利点と制限をすべて備えています。

利点を次に示します。

- 接続はリロード中も持続し、タイムアウトしません。
- ASASM リロード中も接続を維持でき、スタートアップ メッセージが表示されます。
- ASASM がイメージをロードできない場合、ROMMON にアクセスできます。

制限を次に示します。

- 接続が低速です（9600 ボー）。
- 一度にアクティブにできるコンソール接続は 1 つだけです。

（注） 接続は保持されるため、ASASM を正しくログアウトしないと、意図したよりも長く接続が存続する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。詳細については、「CLI 設定ガイド」を参照してください。

例

次に、スロット 3 の ASASM にコンソール アクセスする例を示します。

```
Router# service-module session slot 3
ciscoasa>
```

関連コマンド

コマンド	説明
session	バックプレーン経由で ASASM に Telnet 接続します。

session

スイッチの CLI から ASASM にバックプレーン経由で Telnet 接続するには、特権 EXEC モードで **session** コマンドを使用します。

session [**switch** {**1** | **2**}] **slot** *number* **processor 1**

構文の説明

processor 1	プロセッサ番号を指定します。これは常に 1 です。
slot *number*	スロット番号を指定します。モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。
switch {**1** | **2**}	（オプション）VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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

特権 EXEC

使用上のガイドライン

session コマンドを使用して、ASASM への Telnet 接続を作成します。

利点を次に示します。

- ASASM への複数のセッションを同時に使用できます。
- Telnet セッションは、高速接続です。

制限を次に示します。

- Telnet セッションは、ASASM リロード時に終了し、タイムアウトします。
- 完全にロードするまで ASASM にアクセスできません。したがって、ROMMON にアクセスできません。

（注） **session** *slot* **processor 0** コマンドは、他のサービス モジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。

ログイン パスワードの入力が求められます。ASASM にログイン パスワードを入力します。デフォルトのパスワードは、**cisco** です。

ユーザ EXEC モードにアクセスします。

例

次の例では、プロセッサ 1 の ASASM への Telnet 接続を確立します。

```
Router# session slot number processor 1
ciscoasa passwd: cisco
ciscoasa>
```

関連コマンド

コマンド	説明
service-module session	スイッチの CLI から ASASM へのコンソール アクセスを取得します。

show boot device

デフォルトの起動パーティションを表示するには、**show boot device** コマンドを使用します。

show boot device [*mod_num*]

構文の説明

mod_num	（任意）モジュール番号を指定します。インストールされたモジュールとその番号を表示するには、**show module** コマンドを使用します。

デフォルト

デフォルトの起動パーティションは cf:4 です。

コマンド モード

特権 EXEC

例

次に、Cisco IOS ソフトウェア上でインストール済みの各 ASA の起動パーティションを表示する **show boot device** コマンドの出力例を示します。

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

関連コマンド

コマンド	説明
boot device (IOS)	デフォルトの起動パーティションを設定します。
show module (IOS)	インストールされているすべてのモジュールを表示します。

show diagnostic loopback

テスト実行数、受信したループバック パケット数、検出された障害数などの PC のループバック テストに関連する情報を表示するには、特権 EXEC モードで **show diagnostics loopback** コマンドを使用します。

show diagnostics loopback

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	トランスペアレント	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
12.2(18)SXF5	このコマンドが追加されました。

使用上のガイドライン

show diagnostics loopback コマンドは、テスト実行数、受信したループバック パケット数、検出された障害数などの PC のループバック テストに関連する情報を提供します。

例

次に、**show diagnostics loopback** コマンドの出力例を示します。

```
ciscoasa# show diagnostics loopback

Port    Test    Pkts-received  Failures
0       447     447            0
1       447     447            0
```

関連コマンド

コマンド	説明
clear diagnostics loopback	オンライン診断テストの設定をクリアします。
firewall autostate	自動ステート機能をイネーブルにします。

show firewall autostate

自動ステート機能の設定を表示するには、特権 EXEC モードで **show firewall autostate** コマンドを使用します。

show firewall autostate

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

デフォルトでは、自動ステート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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

使用上のガイドライン

Cisco IOS ソフトウェアの自動ステート メッセージ機能により、スイッチ インターフェイスに障害があるのか起動しているのかを ASA が迅速に検出できます。次の場合に、スイッチのスーパーバイザから ASA に自動ステート メッセージが送信されます。

- VLAN に属している最後のインターフェイスが停止した
- VLAN に属している最初のインターフェイスが動作を開始した

関連コマンド

コマンド	説明
clear diagnostics loopback	オンライン診断テストの設定をクリアします。
firewall autostate	自動ステート機能をイネーブルにします。

show firewall module

各 ASA に割り当てられた VLAN グループを表示するには、特権 EXEC モードで **show firewall module** コマンドを入力します。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*]

構文の説明

module_number	(任意)モジュール番号を指定します。インストールされたモジュールとその番号を表示するには、**show module** コマンドを使用します。
switch {**1**	**2**}	(オプション)VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、すべての VLAN グループを示す **show firewall module** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN を VLAN グループに割り当てます。
show firewall module vlan-group	VLAN グループと、これに割り当てられた VLAN を表示します。
show module	インストールされているすべてのモジュールを表示します。

show firewall module state

各 ASA の状態を表示するには、特権 EXEC モードで **show firewall module state** コマンドを入力します。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **state**

構文の説明

module_number	(任意)モジュール番号を指定します。
switch {**1** | **2**}	(オプション)VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、**show firewall module state** コマンドの出力例を示します。

```
Router# show firewall module 11 state
Firewall module 11:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN を VLAN グループに割り当てます。
show firewall module vlan-group	VLAN グループと、これに割り当てられた VLAN を表示します。
show module	インストールされているすべてのモジュールを表示します。

show firewall module traffic

各 ASA を通過するトラフィックを表示するには、特権 EXEC モードで **show firewall module traffic** コマンドを入力します。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **traffic**

構文の説明

module_number	(任意)モジュール番号を指定します。
switch {**1** | **2**}	(オプション)VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、**show firewall module traffic** コマンドの出力例を示します。

```
Router# show firewall module 11 traffic
Firewall module 11:

Specified interface is up line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
```

```
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN を VLAN グループに割り当てます。
show firewall module vlan-group	VLAN グループと、これに割り当てられた VLAN を表示します。
show module	インストールされているすべてのモジュールを表示します。

show firewall module version

ASA サービス モジュール のソフトウェア バージョン番号を表示するには、特権 EXEC モードで **show firewall module version** コマンドを使用します。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **version**

構文の説明

module_number	(任意)モジュール番号を指定します。
switch {**1** | **2**}	(オプション)VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

例

次に、**show firewall module version** コマンドの出力例を示します。

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN のグループを作成します。
show module	インストールされているすべてのモジュールを表示します。

show firewall module vlan-group

ASA に割り当て可能な VLAN グループを表示するには、特権 EXEC モードで **show firewall module vlan-group** コマンドを入力します。

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **vlan-group** [*firewall_group*]

構文の説明

firewall_group	（任意）グループ ID を指定します。
module_number	（任意）モジュール番号を指定します。
switch {**1** | **2**}	（オプション）VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、**show firewall module vlan-group** コマンドの出力例を示します。

```
Router# show firewall module vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN のグループを作成します。
show module	インストールされているすべてのモジュールを表示します。

show firewall multiple-vlan-interfaces

ASASM の複数のファイアウォール VLAN インターフェイスの状態を表示するには、特権 EXEC モードで **show firewall multiple-vlan-interfaces** コマンドを入力します。

show firewall multiple-vlan-interfaces

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、**show firewall multiple-vlan-interfaces** コマンドの出力例を示します。

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN のグループを作成します。
show module	インストールされているすべてのモジュールを表示します。

show module

スイッチが ASASM を許可し、オンラインにしたことを確認するには、特権 EXEC モードで **show module** コマンドを使用します。

show module [**switch** {**1** | **2**}] [*mod-num* | **all**]

構文の説明

all	(オプション)すべてのモジュールを指定します。
mod_num	(任意)モジュール番号を指定します。
switch {**1**	**2**}	(オプション)VSS のコンフィギュレーションの場合は、スイッチ番号を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

例

次に、**show module** コマンドの出力例を示します。

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok
```

```
Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

関連コマンド

コマンド	説明
firewall module	VLAN グループを ASA に割り当てます。
firewall vlan-group	VLAN のグループを作成します。

パート 3

参照先

CHAPTER 7

コマンドライン インターフェイスの使用

この章では、ASA での CLI の使用方法について説明します。次の項目を取り上げます。

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

ファイアウォール モードとセキュリティ コンテキスト モード

ASA は、次のモードの組み合わせで動作します。

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

  ファイアウォール モードは、ASA がレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを決定します。

- マルチ コンテキスト モードまたはシングル コンテキスト モード

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

特定のモードでしか使用できないコマンドもあります。

コマンドのモードとプロンプト

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

（注） さまざまなタイプのプロンプトはすべてデフォルトで、別々のプロンプトとして設定できます。

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

  ```
  ciscoasa
  ```

- プロンプト文字列を印刷するときに、プロンプト コンフィギュレーションが解析され、設定されたキーワード値が **prompt** コマンドで設定された順に印刷されます。キーワード引数は、ホスト名、ドメイン、コンテキスト、プライオリティ、状態のいずれかで、任意の順になります。

  ```
  asa(config)# prompt hostname context priority state
  ```

- コンテキスト内では、プロンプトはホスト名の後にコンテキスト名が表示されます。

  ```
  ciscoasa/context
  ```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

  ユーザ EXEC モードでは、最小限の ASA 設定が表示されます。ユーザ EXEC モードのプロンプトは、初めて ASA にアクセスしたときに次のように表示されます。

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 特権 EXEC モード

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

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- グローバル コンフィギュレーション モード

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

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- コマンド固有のコンフィギュレーション モード

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

  ```
  ciscoasa(config-if)#

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

構文の書式

コマンド構文の説明では、表 7-1 に記載されている表記法を使用します。

表 7-1　構文の表記法

表記法	説明
ボールド	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素(キーワードまたは引数)は、角かっこで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表 7-1　構文の表記法（続き）

表記法	説明
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの短縮形

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

コマンドラインの編集

ASA では、Cisco IOS ソフトウェアと同じコマンドライン編集ルールが使用されます。**show history** コマンドを使用して以前入力した全コマンドを表示することも、↑ キーまたは **^p** コマンドで 1 つずつ前のコマンドを表示することもできます。前に入力したコマンドを確認したら、↓ キーまたは **^n** コマンドでリスト内で前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、**Enter** キーを押して実行することもできます。**^w** でカーソルの左側にある単語を削除することも、**^u** でカーソルのある行を消去することもできます。

ASA では、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

コマンドの完成

部分的な文字列を入力してからコマンドまたはキーワードを完成させるには、**Tab** キーを押します。ASA は、部分的な文字列がコマンドまたはキーワード 1 つだけと一致する場合に限り、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して **Tab** キーを押した場合は、一致するコマンドが複数あるため、ASA はコマンドを完成させません。一方、**dis** と入力して Tab キーを押すと、コマンド **disable** が完成します。

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*

  特定のコマンドのヘルプを表示します。

- *command_name* **?**

  使用可能な引数のリストを表示します。

- *string*?（スペースなし）

  その文字列で始まるコマンドをリストします。

- **?** および **+?**

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

(注) コマンド文字列に疑問符(?)を組み込む場合は、誤って CLI ヘルプを起動しないよう、疑問符を入力する前に **Ctrl+V** を押す必要があります。

実行コンフィギュレーションの表示

実行コンフィギュレーションを表示するには、次のいずれかのコマンドを使用します。

コマンド出力をフィルタリングするには、「show コマンドと more コマンドの出力のフィルタリング」セクション(7-5 ページ)を参照してください。

コマンド	目的
show running-config [**all**] [*command*]	実行コンフィギュレーションを表示します。**all** を指定すると、すべてのデフォルト設定も表示されます。*command* を指定すると、関連するコマンドだけが出力に含まれます。 (注) 多くのパスワードは ***** として表示されます。パスワードをプレーン テキストで表示するか、またはマスター パスフレーズがイネーブルの場合に暗号化された形式で表示するには、次の **more** コマンドを使用します。
more system:running-config	実行コンフィギュレーションを表示します。パスワードはプレーン テキストで表示されるか、またはマスター パスフレーズがイネーブルの場合は暗号化された形式で表示されます。

show コマンドと more コマンドの出力のフィルタリング

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

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

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

または

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

(注) **more** コマンドは、実行コンフィギュレーションだけではなく、任意のファイルのコンテンツを表示できます。詳細については、コマンド リファレンスを参照してください。

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

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

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

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

疑問符(?)やタブなど、CLI の特殊文字をすべてエスケープするには、**Ctrl+V** を使用します。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

show コマンド出力のリダイレクトと追加

show コマンドの出力を画面に表示するのではなく、デバイス上またはリモート ロケーション内のファイルにリダイレクトすることができます。デバイス上のファイルへのリダイレクトの場合は、ファイルにコマンド出力を追加することもできます。

show *command* **|** {**append** | **redirect**} *url*

- **append** *url* により、出力が既存のファイルに追加されます。次のいずれかを使ってファイルを指定します。
  - **disk0:/**[[*path*/]*filename*] または **flash:/**[[*path*/]*filename*]:**flash** と **disk0** の両方が内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path*/]*filename*]:外部メモリを示します。
- **redirect** *url* により、指定されたファイルが作成されます。または、ファイルがすでに存在している場合は、上書きされます。
  - **disk0:/**[[*path*/]*filename*] または **flash:/**[[*path*/]*filename*]:**flash** と **disk0** の両方が内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path*/]*filename*]:外部メモリを示します。
  - **smb:/**[[*path*/]*filename*]:サーバ メッセージ ブロック、UNIX サーバのローカル ファイル システムを示します。
  - **ftp://**[[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*]]:FTP サーバを示します。**type** には次のいずれかのキーワードを使用できます。**ap**(ASCII パッシブ モード)、**an**(ASCII ノーマル モード)、**ip**(デフォルト:バイナリ パッシブ モード)、**in**(バイナリ ノーマル モード)。

– **scp://**[[*user*[**:***password*]@]*server*[**/***path*]**/***filename*[**;int=***interface_name*]]：SCP サーバを示します。**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定のインターフェイスを使用してセキュア コピー（SCP）サーバに接続するようになります。

– **tftp://**[[*user*[**:***password*]@]*server*[**:***port*]**/**[*path***/**]*filename*[**;int=***interface_name*]]：TFTP サーバを示します。

show コマンド出力の行数の取得

実際の **show** コマンド出力を表示するのではなく、出力の行数のみを確認したり、正規表現に一致する行数のみを確認したりすることもできます。それにより、行数を以前のコマンド入力時の数と簡単に比較することができます。この方法は、設定に変更を加えたときの簡易チェックとして使用できます。**count** キーワードを使用するか、**grep** キーワードに **-c** を追加します。

show *command* **| count** [*regular_expression*]

show *command* **| grep -c** [*regular_expression*]

regular_expression には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。正規表現はオプションです。正規表現を含めない場合に返されるカウントは、フィルタリングされていない出力の合計行数となります。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、メタ文字と呼ばれる特定のキーボード文字は、正規表現で使用されると、特別な意味を持ちます。疑問符（?）やタブなど、CLI の特殊文字をすべてエスケープするには、**Ctrl+V** を使用します。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

たとえば、**show running-config** の出力のすべての行の合計数を表示するには、以下のように行います。

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

下記の例は、稼働中のインターフェイスの数をすばやく確認できる方法を示しています。最初の例は、正規表現で **grep** キーワードを使用することにより、稼動状態を示す行のみに絞り込む方法です。次の例は、**-c** オプションを追加することにより、実際の出力行ではなくその数だけを表示する方法です。

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

コマンド出力のページング

help または **?**、**show**、**show xlate** など、長いリストが出力されるコマンドでは、1 画面分ずつ表示して停止させるか、リストの最後まで表示させるかを決めることができます。**pager** コマンドを使用すると、画面上に表示する行数を選択して、その行数を表示した後に More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

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

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

- 次の 1 画面分の情報を表示するには、**スペース** バーを押します。
- 次の行を表示するには、**Enter** キーを押します。
- コマンドラインに戻るには、**q** キーを押します。

コメントの追加

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

テキスト コンフィギュレーション ファイル

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

テキスト ファイルでコマンドと行が対応する仕組み

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

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

```
ciscoasa(config)# context a
```

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

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

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

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト入力

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

行の順序

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

テキスト コンフィギュレーションに含まれないコマンド

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

パスワード

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

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

マルチセキュリティ コンテキスト ファイル

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

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、ASA の基本設定を示すシステム コンフィギュレーション
- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

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

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

サポートされている文字セット

ASA CLI は、現在 UTF-8 の符号化方式だけをサポートしています。UTF-8 は Unicode 文字の特定の符号化スキームであり、ASCII 文字のサブセットと互換性を持つように設計されています。ASCII 文字は UTF-8 で 1 バイト文字として表現されます。その他のすべての文字は、UTF-8 でマルチバイト文字として表現されます。

ASCII の印刷可能文字(0x20 ～ 0x7e)はすべてサポートされています。印刷可能な ASCII 文字は、ISO 8859-1 の文字と同じです。UTF-8 は ISO 8859-1 のスーパーセットであるため、最初の 256 文字(0 ～ 255)は ISO 8859-1 の文字と同じになります。ASA CLI は、ISO 8859-1 の文字を 255 文字(マルチバイト文字)までサポートしています。