CHAPTER 24

same-security-traffic コマンド～ show asdm sessions コマンド

same-security-traffic

同じセキュリティ レベルのインターフェイス間での通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可するには、グローバル コンフィギュレーション モードで **same-security-traffic** コマンドを使用します。同じセキュリティ レベルのトラフィック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。

same-security-traffic permit {**inter-interface | intra-interface**}

no same-security-traffic permit {**inter-interface | intra-interface**}

構文の説明

inter-interface	同じセキュリティ レベルを持つ異なるインターフェイス間での通信を許可します。
intra-interface	同じインターフェイスに入って同じインターフェイスから出る通信を許可します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**intra-interface** キーワードで、IPSec トラフィックだけでなくすべてのトラフィックが、同じインターフェイスに入って同じインターフェイスから出ることが許可されるようになりました。

使用上のガイドライン

同じセキュリティ レベルのインターフェイス間での通信を許可すると（**same-security-traffic inter-interface** コマンドを使用してイネーブルにします）、次の利点があります。

- 101 より多い数の通信インターフェイスを設定できます。各インターフェイスで異なるレベルを使用する場合は、レベルごと（0 ～ 100）に 1 つのインターフェイスのみを設定できます。
- アクセス リストなしで、すべての同じセキュリティ レベルのインターフェイス間で自由にトラフィックを送受信できます。

same-security-traffic intra-interface コマンドを使用すると、トラフィックが同じインターフェイスに入って同じインターフェイスから出ることができます。この動作は、通常は許可されていません。この機能は、あるインターフェイスに入り、その後同じインターフェイスからルーティングされる VPN トラフィックの場合に役立ちます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネット

ワークがあり、セキュリティ アプライアンスがハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックはセキュリティ アプライアンスに入ってから他のスポークに再度ルーティングされる必要があります。

（注）　**same-security-traffic intra-interface** コマンドによって許可されるすべてのトラフィックには、引き続きファイアウォール ルールが適用されます。リターン トラフィックがセキュリティ アプライアンスを通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

例

次に、同じセキュリティ レベルのインターフェイス間での通信をイネーブルにする例を示します。

```
hostname(config)# same-security-traffic permit inter-interface
```

次に、トラフィックが同じインターフェイスに入って同じインターフェイスから出られるようにする例を示します。

```
hostname(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
show running-config same-security-traffic	**same-security-traffic** コンフィギュレーションを表示します。

sasl-mechanism

LDAP クライアントを LDAP サーバに対して認証するための Simple Authentication and Security Layer（SASL）メカニズムを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sasl-mechanism** コマンドを使用します。SASL 認証メカニズムのオプションは、**digest-md5** および **kerberos** です。

認証メカニズム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。

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

（注） VPN ユーザにとっては、セキュリティ アプライアンスが LDAP サーバへのクライアント プロキシとして動作するため、ここでの LDAP クライアントとはセキュリティ アプライアンスを意味しています。

構文の説明

digest-md5	セキュリティ アプライアンスは、ユーザ名とパスワードから計算された MD5 値を使用して応答します。
kerberos	セキュリティ アプライアンスは、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信することによって応答します。
server-group-name	最大 64 文字の Kerberos AAA サーバ グループを指定します。

デフォルト

デフォルトの動作や値はありません。セキュリティ アプライアンスは、認証パラメータをプレーン テキストで LDAP サーバに渡します。

（注） SASL を設定していない場合は、**ldap-over-ssl** コマンドを使用して、SSL によって LDAP 通信を保護することを推奨します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが SASL メカニズムを使用して LDAP サーバに対する認証を行うよう指定するには、このコマンドを使用します。

セキュリティ アプライアンスと LDAP サーバの両方で、複数の SASL 認証メカニズムをサポートできます。SASL 認証をネゴシエートする場合、セキュリティ アプライアンスはサーバに設定されている SASL メカニズムのリストを取得して、セキュリティ アプライアンスとサーバの両方に設定されているメカニズムのうち最も強力な認証メカニズムを設定します。Kerberos メカニズムは、Digest-MD5 メカニズムよりも強力です。たとえば、LDAP サーバとセキュリティ アプライアンスの両方でこれら 2 つのメカニズムがサポートされている場合、セキュリティ アプライアンスでは、より強力な Kerberos メカニズムが選択されます。

各メカニズムは独立して設定されるため、SASL メカニズムをディセーブルにするには、ディセーブルにする各メカニズムに対して別々に **no** コマンドを入力する必要があります。明示的にディセーブルにしないメカニズムは引き続き有効です。たとえば、両方の SASL メカニズムをディセーブルにするには、次の両方のコマンドを入力する必要があります。

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

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、名前が ldapsvr1、IP アドレスが 10.10.0.1 の LDAP サーバに対する認証のために SASL メカニズムをイネーブルにする例を示します。この例では、SASL digest-md5 認証メカニズムがイネーブルにされています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
```

次に、SASL Kerberos 認証メカニズムをイネーブルにして、Kerberos AAA サーバとして kerb-servr1 を指定する例を示します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
server-type	LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

sast

CTL レコードに作成する SAST 証明書の数を指定するには、CTL ファイル コンフィギュレーション モードで **sast** コマンドを使用します。CTL ファイル内の SAST 証明書の数をデフォルト値の 2 に戻すには、このコマンドの **no** 形式を使用します。

sast *number_sasts*

no sast *number_sasts*

構文の説明

number_sasts	作成する SAST キーの数を指定します。デフォルトは 2 です。指定できる最大数は 5 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	透過	シングル	コンテキスト	システム
CTL ファイル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

CTL ファイルは、System Administrator Security Token（SAST; システム管理者セキュリティ トークン）によって署名されます。

電話プロキシは CTL ファイルを生成するため、CTL ファイル自体を署名するための SAST キーを作成する必要があります。このキーは、セキュリティ アプライアンスで生成できます。SAST は、自己署名証明書として作成されます。

通常、CTL ファイルには複数の SAST が含まれています。ある SAST が回復可能でない場合は、後でもう 1 つの SAST を使用してファイルを署名できます。

例

次に、**sast** コマンドを使用して、CTL ファイルに 5 つの SAST 証明書を作成する例を示します。

```
hostname(config-ctl-file)# sast 5
```

関連コマンド

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

secondary

フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを付与するには、フェールオーバー グループ コンフィギュレーション モードで **secondary** 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** 形式を入力します。

secondary

no secondary

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

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** 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	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリ プライオリティをフェールオーバー グループに割り当てることによって、両方のユニットが同時（ユニットのポーリング タイム内）に起動したときにフェールオーバー グループがアクティブになるユニットを指定します。あるユニットがもう一方のユニットよりも先にブートした場合、両方のフェールオーバー グループがそのユニットでアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
```

```
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。
primary	プライマリ ユニットに、セカンダリ ユニットよりも高いプライオリティを付与します。

secondary-color

WebVPN ログイン、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 カラーを設定するには、webvpn モードで **secondary-color** コマンドを使用します。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。

secondary-color [*color***]**

no secondary-color

構文の説明

color	（任意）色を指定します。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。 • 名前の最大長は 32 文字です。

デフォルト

デフォルトのセカンダリ カラーは HTML の #CCCCFF（薄紫色）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、そのうちの 40 色は MAC と PC とでは異なった表示になります。最適な結果を得るために、公開されている RGB テーブルをチェックしてください。RGB テーブルをオンラインで検索するには、検索エンジンで RGB と入力します。

例

次に、HTML の色値 #5F9EAO（灰青色）を設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

関連コマンド

コマンド	説明
title-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 バーの色を設定します。

secondary-text-color

WebVPN ログイン、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するには、webvpn モードで **secondary-text-color** コマンドを使用します。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。

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

no secondary-text-color

構文の説明

auto	text-color コマンドの設定に基づいて、黒または白が選択されます。つまり、プライマリ カラーが黒の場合、この値は白になります。
black	デフォルトのセカンダリ テキストの色は黒です。
white	テキストの色を白に変更できます。

デフォルト

デフォルトのセカンダリ テキストの色は黒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、セカンダリ テキストの色を白に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

関連コマンド

コマンド	説明
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 バーのテキストの色を設定します。

secure-unit-authentication

セキュア ユニット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 **secure-unit-authentication enable** コマンドを使用します。セキュア ユニット認証をディセーブルにするには、**secure-unit-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セキュア ユニット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。このオプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにクライアントに対してユーザ名 / パスワード認証を要求することによって、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。

（注） この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

secure-unit-authentication {**enable** | **disable**}

no secure-unit-authentication

構文の説明

disable	セキュア ユニット認証をディセーブルにします。
enable	セキュア ユニット認証をイネーブルにします。

デフォルト

セキュア ユニット認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネル グループに認証サーバ グループが設定されている必要があります。

プライマリセキュリティ アプライアンスでセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証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、セキュア ユニット認証をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-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	イネーブルの場合、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットがユーザ認証の前に VPN トンネルを通過できます。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。
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、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

security-level

インターフェイスのセキュリティ レベルを設定するには、インターフェイス コンフィギュレーション モードで **security-level** コマンドを使用します。セキュリティ レベルをデフォルトに設定するには、このコマンドの **no** 形式を使用します。セキュリティ レベルを指定すると、高いセキュリティ レベルのネットワークと低いセキュリティ レベルのネットワークとの間の通信に追加の保護が設定され、高いセキュリティ レベルのネットワークが低いセキュリティ レベルのネットワークから保護されます。

security-level *number*

no security-level

構文の説明

number	0（最低）～ 100（最高）の整数。

デフォルト

デフォルトのセキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を指定して、明示的にセキュリティ レベルを設定しないと、セキュリティ アプライアンスによってセキュリティ レベルが 100 に設定されます（**nameif** コマンドを参照）。このレベルは必要に応じて変更できます。

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	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**nameif** 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 モードのコマンドに変更されました。

使用上のガイドライン

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のインスペクション エンジンは、セキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。

  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - OraServ インスペクション エンジン：ホストのペア間に OraServ ポートへの制御接続が存在する場合は、セキュリティ アプライアンス経由での着信データ接続のみが許可されます。
- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。
- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

通常、同じセキュリティ レベルのインターフェイス間では通信できません。同じセキュリティ レベルのインターフェイス間で通信する場合は、**same-security-traffic** コマンドを参照してください。101 を超える通信インターフェイスを作成する必要がある場合や、2 つのインターフェイス間のトラフィックに同じ保護機能を適用する必要がある場合（同程度のセキュリティが必要な 2 つの部門がある場合など）に、2 つのインターフェイスに同じレベルを割り当てて、それらのインターフェイス間での通信を許可できます。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

例

次に、2 つのインターフェイスのセキュリティ レベルを 100 と 0 に設定する例を示します。

```
hostname(config)# interface gigabitethernet0/0
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear local-host	すべての接続をリセットします。
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。

コマンド	説明
nameif	インターフェイス名を設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

send response

RADIUS の Accounting-Response Start および Accounting-Response Stop メッセージを RADIUS の Accounting-Request Start および Stop メッセージの送信元に送信するには、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 **send response** 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します。

このオプションは、デフォルトで無効です。

send response

no send response

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、RADIUS アカウンティングで応答を送信する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

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。
parameters	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。

seq-past-window

パストウィンドウ シーケンス番号（TCP 受信ウィンドウの適切な境界を越える受信 TCP パケットのシーケンス番号）を持つパケットに対するアクションを設定するには、tcp マップ コンフィギュレーション モードで **seq-past-window** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

seq-past-window {**allow** | **drop**}

no seq-past-window

構文の説明

allow	パストウィンドウ シーケンス番号を持つパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。
drop	パストウィンドウ シーケンス番号を持つパケットをドロップします。

デフォルト

デフォルトのアクションでは、パストウィンドウ シーケンス番号を持つパケットはドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

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

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **seq-past-window**：tcp マップ コンフィギュレーション モードでは、**seq-past-window** コマンドおよびその他数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、パストウィンドウ シーケンス番号を持つパケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# seq-past-window allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

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

serial-number

登録時に、セキュリティ アプライアンスのシリアル番号を証明書に含めるには、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 **serial-number** 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。

serial-number

no serial-number

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、シリアル番号は含まれません。

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	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

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、トラストポイント central の登録要求にセキュリティ アプライアンスのシリアル番号を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
```

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。

server

デフォルトの電子メール プロキシ サーバを指定するには、該当する電子メール プロキシ モードで **server** 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。セキュリティ アプライアンスは、ユーザがサーバを指定せずに電子メール プロキシに接続した場合、デフォルトの電子メール サーバに要求を送信します。デフォルトのサーバを設定せず、ユーザもサーバを指定しない場合、セキュリティ アプライアンスではエラーが返されます。

server {*ipaddr or hostname*}

no server

構文の説明

hostname	デフォルトの電子メール プロキシ サーバの DNS 名。
ipaddr	デフォルトの電子メール プロキシ サーバの IP アドレス。

デフォルト

デフォルトでは、デフォルトの電子メール プロキシ サーバはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、10.1.1.7 という IP アドレスを持つ POP3S 電子メール サーバを設定する 例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server（tls プロキシ）

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS プロキシ コンフィギュレーション モードで **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。

server trust-point *p_tp*

no server trust-point *p_tp*

構文の説明

trust-point *p_tp*	定義されているトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

TLS プロキシで TLS サーバ ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを制御するには、TLS プロキシ コンフィギュレーション モードで **server** コマンドを使用します。TLS ハンドシェイク時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。この値は、**crypto ca trustpoint** コマンドで定義したトラストポイントに対応します。自己署名証明書、または認証局に登録された証明書を指定できます。

server コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

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。

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

関連コマンド

コマンド	説明
client	TLS プロキシで TLS クライアント ロールを持つセキュリティ アプライアンスの TLS ハンドシェイク パラメータを設定します。
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。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

server authenticate-client

TLS ハンドシェイク時におけるセキュリティ アプライアンスでの TLS クライアントの認証をイネーブルにするには、TLS プロキシ コンフィギュレーション モードで **server authenticate-client** コマンドを使用します。

クライアント認証をバイパスするには、このコマンドの **no** 形式を使用します。

server authenticate-client

no server authenticate-client

構文の説明

このコマンドには、キーワードや引数はありません。

デフォルト

このコマンドは、デフォルトでイネーブルです。つまり、セキュリティ アプライアンスとのハンドシェイク時に、TLS クライアントは、証明書の提示を要求されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TLS プロキシ ハンドシェイク時にクライアント認証が必要であるかどうかを制御するには、**server authenticate-client** コマンドを使用します。イネーブルの場合（デフォルト）、セキュリティ アプライアンスは TLS クライアントに証明書要求 TLS ハンドシェイク メッセージを送信し、TLS クライアントは証明書の提示を要求されます。

クライアント認証をディセーブルにするには、このコマンドの **no** 形式を使用します。TLS クライアント認証のディセーブルは、セキュリティ アプライアンスが CUMA クライアントや、Web ブラウザなどのクライアント証明書を送信できないクライアントと相互運用する必要がある場合に適しています。

例

次に、クライアント認証をディセーブルにした TLS プロキシ インスタンスを設定する例を示します。

```
hostname(config)# tls-proxy mmp_tls
hostname(config-tlsp)# no server authenticate-client
hostname(config-tlsp)# server trust-point cuma_server_proxy
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを設定します。

server-port

ホストの AAA サーバ ポートを設定するには、AAA サーバ ホスト モードで **server-port** コマンドを使用します。指定されているサーバ ポートを削除するには、このコマンドの **no** 形式を使用します。

server-port *port-number*

no server-port

構文の説明

port-number	0 ～ 65535 の範囲のポート番号。

デフォルト

デフォルトのサーバ ポートは次のとおりです。

- SDI：5500
- LDAP：389
- Kerberos：88
- NT：139
- TACACS+：49

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「srvgrp1」という名前の SDI AAA サーバでサーバ ポート番号 8888 を使用するように設定する例を示します。

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ パラメータを設定します。

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

server-separator

電子メール サーバ名および VPN サーバ名のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **server-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの no 形式を使用します。

server-separator {*symbol*}

no server-separator

構文の説明

symbol	電子メール サーバ名および VPN サーバ名を区切る文字。選択肢は「@」（アット マーク）、「|」（パイプ）、「:（コロン）」、「|（ハッシュ）」、「,（カンマ）」、「;」（セミコロン）です。

デフォルト

デフォルトは「@」（アットマーク）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

サーバの区切り文字には、名前の区切り文字とは異なる文字を使用する必要があります。

例

次に、パイプ（|）を IMAP4S サーバの区切り文字として設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

関連コマンド

コマンド	説明
name-separator	電子メールおよび VPN のユーザ名とパスワードを区切ります。

server-type

LDAP サーバ モデルを手動で設定するには、AAA サーバ ホスト コンフィギュレーション モードで **server-type** コマンドを使用します。セキュリティ アプライアンスでは、次のサーバ モデルがサポートされています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前の Sun ONE Directory Server）
- LDAPv3 に準拠した一般的な LDAP ディレクトリ サーバ（パスワード管理なし）

このコマンド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。

server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

no server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

構文の説明

auto-detect	セキュリティ アプライアンスで自動検出によって LDAP サーバ タイプを決定することを指定します。
generic	Sun および Microsoft の LDAP ディレクトリ サーバ以外の LDAP v3 準拠のディレクトリ サーバを指定します。一般的な LDAP サーバでは、パスワード管理はサポートされません。
microsoft	LDAP サーバが Microsoft Active Directory であることを指定します。
openldap	LDAP サーバが OpenLDAP サーバであることを指定します。
novell	LDAP サーバが Novell サーバであることを指定します。
sun	LDAP サーバが Sun Microsystems JAVA System Directory Server であることを指定します。

デフォルト

デフォルトでは、自動検出によってサーバ タイプの決定が試みられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。
8.0(2)	OpenLDAP および Novell サーバ タイプのサポートが追加されました。

使用上のガイドライン

セキュリティ アプライアンスは LDAP バージョン 3 をサポートしており、Sun Microsystems JAVA System Directory Server、Microsoft Active Directory、およびその他の LDAPv3 ディレクトリ サーバと互換性があります。

（注）

- Sun : Sun ディレクトリ サーバにアクセスするためにセキュリティ アプライアンスに設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory を使用したパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- Generic：パスワード管理機能はサポートされていません。

デフォルトで、セキュリティ アプライアンスでは、Microsoft ディレクトリ サーバ、Sun LDAP ディレクトリ サーバ、または一般的な LDAPv3 サーバのいずれに接続しているかが自動検出されます。ただし、自動検出で LDAP サーバ タイプを決定できない場合で、サーバが Microsoft または Sun のサーバであることが明らかである場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバとして手動で設定できます。

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、IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 のサーバ タイプを設定する例を示します。この最初の例では、Sun Microsystems LDAP サーバを設定しています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
```

次に、セキュリティ アプライアンスで自動検出を使用してサーバ タイプを決定することを指定する例を示します。

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。
sasl-mechanism	LDAP クライアントおよびサーバ間での SASL 認証を設定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

server trust-point

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS サーバ コンフィギュレーション モードで **server trust-point** コマンドを使用します。

server trust-point *proxy_trustpoint*

構文の説明

proxy_trustpoint	**crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントでは、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**server trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

server trust-point コマンドは、TLS ハンドシェイク時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。証明書は、セキュリティ アプライアンス が所有している必要があります（ID 証明書）。証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。

接続を開始できる各エンティティに対して TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、TLS クライアントのロールを担います。TLS プロキシにはクライアント プロキシとサーバ プロキシが厳密に定義されているため、いずれのエンティティからも接続が開始される可能性がある場合には、2 つの TLS プロキシ インスタンスを定義する必要があります。

（注） 電話プロキシとともに使用する TLS プロキシ インスタンスを作成する場合、サーバのトラストポイントは、CTL ファイル インスタンスによって作成される内部電話プロキシ トラストポイントです。トラストポイント名は、*internal_PP_<ctl-file_instance_name>* の形式となります。

例

次に、**server trust-point** コマンドを使用して、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定する例を示します。

```
hostname(config-tlsp)# server trust-point ent_y_proxy
```

関連コマンド

コマンド	説明
client（TLS プロキシ）	TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。
client 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。
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。
tls-proxy	TLS プロキシ インスタンスを設定します。

service

拒否された TCP 接続のリセッ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 **service** コマンドを使用します。リセッ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。

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

構文の説明

interface *interface_name*	指定したインターフェイスのリセットをイネーブルまたはディセーブルにします。
resetinbound	セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否されたすべての着信 TCP セッションに TCP リセットを送信します。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。インターフェイスを指定しない場合、この設定はすべてのインターフェイスに適用されます。
resetoutbound	セキュリティ アプライアンスの通過を試み、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否されたすべての発信 TCP セッションに TCP リセットを送信します。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、セキュリティ アプライアンスは拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。
resetoutside	最もセキュリティ レベルの低いインターフェイスで終端し、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスによって拒否された TCP パケットのリセットをイネーブルにします。このセキュリティ アプライアンスは、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、セキュリティ アプライアンスは拒否されたパケットを何も通知せずに廃棄します。インターフェイス PAT では、**resetoutside** キーワードを使用することを推奨します。このキーワードを使用すると、外部 SMTP または FTP サーバからの IDENT をセキュリティ アプライアンスで終了できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。

デフォルト

デフォルトで、すべてのインターフェイスで **service resetoutbound** が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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	**interface** キーワードおよび **resetoutbound** コマンドが追加されました。

使用上のガイドライン　アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセット フラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

例　次に、内部インターフェイスを除くすべてのインターフェイスで発信リセットをディセーブルにする例を示します。

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

次に、DMZ インターフェイスを除くすべてのインターフェイスで着信リセットをイネーブルにする例を示します。

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

次に、外部インターフェイスが終端となる接続でリセットをイネーブルにする例を示します。

```
hostname(config)# service resetoutside
```

関連コマンド

コマンド	説明
show running-config service	サービス コンフィギュレーションを表示します。

service（CTL プロバイダー）

証明書信頼リスト プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** 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。

service port *listening_port*

no service port *listening_port*

構文の説明

port *listening_port*	クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトのポートは 2444 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。ポートは、クラスタ内の CallManager サーバによってリッスンされているポートである必要があります（[CallManager administration] ページの [Enterprise Parameters] で設定）。デフォルトのポートは 2444 です。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
client	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

service password-recovery

パスワードの回復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 **service password-recovery** コマンドを使用します。パスワードの回復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。パスワードの回復はデフォルトでイネーブルですが、不正なユーザがパスワードの回復メカニズムを使用してセキュリティ アプライアンスを侵害できないようにするためにディセーブルにすることができます。

service password-recovery

no service password-recovery

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

パスワードの回復は、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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、パスワードを忘れた場合、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、ROMMON でセキュリティ アプライアンスを起動できます。次に、コンフィギュレーション レジスタを変更することによって、スタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します（**config-register** コマンドを参照）。たとえば、コンフィギュレーション レジスタがデフォルトの 0x1 の場合、**confreg 0x41** コマンドを入力して値を 0x41 に変更します。セキュリティ アプライアンスがリロードされると、デフォルトのコンフィギュレーションがロードされ、デフォルトのパスワードを使用して特権 EXEC モードを開始できます。その後、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にコピーしてスタートアップ コンフィギュレーションをロードし、パスワードをリセットします。最後に、コンフィギュレーション レジスタを元の設定に戻して、以前と同様に起動するようにセキュリティ アプライアンスを設定します。たとえば、グローバル コンフィギュレーション モードで **config-register 0x1** コマンドを入力します。

PIX 500 シリーズ セキュリティ アプライアンスでは、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、モニタ モードでセキュリティ アプライアンスを起動します。その後、PIX パスワード ツールをセキュリティ アプライアンスにダウンロードして、すべてのパスワードおよび **aaa authentication** コマンドを消去します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが ROMMON を開始することを防止でき、コンフィギュレーションも変更されないままとすることができます。ユーザが ROMMON を開始すると、ユーザは、セキュリティ アプライアンスによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、ROMMON を開始できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復は ROMMON の使用と既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。**service password-recovery** コマンドは、コンフィギュレーション ファイルに情報提供の目的でのみ表示されます。CLI プロンプトでこのコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。セキュリティ アプライアンスが起動時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワードの回復をディセーブルにすると、セキュリティ アプライアンスによって設定が変更され、通常どおりにスタートアップ コンフィギュレーションが起動されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザは、PIX パスワード ツールによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、PIX パスワード ツールを使用できません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復は既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（使用可能な場合）をロードします。

例

次に、ASA 5500 シリーズ適応型セキュリティ アプライアンスでパスワードの回復をディセーブルにする例を示します。

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

次に、PIX 500 シリーズ セキュリティ アプライアンスでパスワードの回復をディセーブルにする例を示します。

```
hostname(config)# no service password-recovery
WARNING: Saving "no service password-recovery" in the startup-config will disable password
recovery via the npdisk application.  The only means of recovering from lost or forgotten
passwords will be for npdisk to erase all file systems including configuration files and
images.  You should make a backup of your configuration and have a mechanism to restore
images from the Monitor Mode command line.
```

次に、ASA 5500 シリーズ適応型セキュリティ アプライアンスで、起動時に ROMMON を開始して、パスワードの回復操作を完了する例を示します。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
config-register	リロード時にスタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します。
enable password	イネーブル パスワードを設定します。
password	ログイン パスワードを設定します。

service-policy（クラス）

別のポリシー マップの下に階層型ポリシー マップを適用するには、クラス コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシー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。階層型ポリシーは、シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを実行する場合に QoS トラフィック シェーピングでのみサポートされています。

service-policy *policymap_name*

no service-policy *policymap_name*

構文の説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。**priority** コマンドを含むレイヤ 3/4 ポリシー マップのみを指定できます。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

階層型プライオリティ キューイングは、トラフィック シェーピング キューをイネーブルにするインターフェイスで使用します。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キュー（**priority-queue** コマンド）は使用しません。

階層型プライオリティ キューイングでは、Modular Policy Framework を使用して次のタスクを実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。
3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。

a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。

b. **shape**：トラフィック シェーピングをクラス マップに適用します。

c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシーマップを呼び出します。

4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	ポリシー マップにクラス マップを指定します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
policy-map	クラス マップに対して実行するアクションを指定します。
priority	プライオリティ キューイングをイネーブルにします。
service-policy（グローバル）	インターフェイスにポリシー マップを適用します。
shape	トラフィック シェーピングをイネーブルにします。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

service-policy（グローバル）

すべてのインターフェイスでグローバルに、または特定のインターフェイスでポリシー マップをアクティブにするには、グローバル コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシー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。インターフェイスでポリシーのセットをイネーブルにするには、**service-policy** コマンドを使用します。

service-policy *policymap_name* [**global** | **interface** *intf*]

no service-policy *policymap_name* [**global** | **interface** *intf*]

構文の説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。レイヤ 3/4 ポリシー マップのみを指定できます。インスペクション ポリシー マップ（**policy-map type inspect**）は指定できません。
global	すべてのインターフェイスにポリシー マップを適用します。
interface *intf*	特定のインターフェイスにポリシー マップを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

サービス ポリシーをイネーブルにするには、Modular Policy Framework を使用します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、インスペクションのグローバル ポリシーがあり、TCP 正規化のインターフェイス ポリシーがある場合、インターフェイスに対してインスペクションと TCP 正規化の両方が適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがトラフィックにグローバルに適用されます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト サービス ポリシーには、次のコマンドが含まれています。

```
service-policy global_policy global
```

例

次に、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにする例を示します。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべてのセキュリティ アプライアンス インターフェイスで新しいポリシー new_global_policy をイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	サービス ポリシーの統計情報をクリアします。
service-policy（クラス）	別のポリシー マップの下に階層型ポリシーを適用します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

session

インテリジェント SSM（AIP SSM や CSC SSM など）への Telnet セッションを確立するには、特権 EXEC モードで **session** コマンドを使用します。

session *slot* [**do** | **ip**]

構文の説明

do	*slot* 引数で指定された SSM でコマンドを実行します。Cisco TAC によって指示された場合以外は、**do** キーワードを使用しないでください。
ip	*slot* 引数で指定された SSM のロギング IP アドレスを設定します。Cisco TAC によって指示された場合以外は、**ip** キーワードを使用しないでください。
slot	SSM スロット番号を指定します。この番号は常に 1 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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**do** キーワードおよび **ip** キーワードが追加されました。これらのキーワードは、Cisco TAC によって指示された場合にのみ使用します。

使用上のガイドライン

このコマンドは、SSM がアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl-Shift-6** を押してから **X** キーを押します。

例

次に、スロット 1 の SSM へのセッションを確立する例を示します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

関連コマンド

コマンド	説明
debug session-command	セッションのデバッグ メッセージを表示します。

set connection

ポリシー マップ内のトラフィック クラスに対して接続制限を指定するには、クラス コンフィギュレーション モードで **set connection** コマンドを使用します。これらの指定を削除して、無制限の接続数を許可するには、このコマンドの **no** 形式を使用します。

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

構文の説明

conn-max *n*	許可する TCP または UDP 同時接続最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。たとえば、TCP または UDP の同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。クラスに設定された場合、このキーワードでは、クラス全体で許可される同時接続最大数が制限されます。この場合、1 つの攻撃ホストがすべての接続を使い果たし、クラスにおいてアクセス リストに一致する他のホストが使用できる接続がなくなる可能性があります。
embryonic-conn-max *n*	許可する同時初期接続最大数を 0 ～ 65535 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。
per-client-embryonic-max *n*	クライアントごとに許可する同時初期接続最大数を 0 ～ 65535 の範囲で設定します。クライアントは、セキュリティ アプライアンスから（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、初期接続制限は、アクセス リストに一致するすべてのクライアントの累積初期接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。
per-client-max *n*	クライアントごとに許可する同時接続最大数を 0 ～ 65535 の範囲で設定します。クライアントは、セキュリティ アプライアンスから（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、接続制限は、アクセス リストに一致するすべてのクライアントの累積接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。クラスに設定された場合、このキーワードでは、クラスにおいてアクセス リストに一致する各ホストに許可される同時接続最大数が制限されます。
random-sequence-number {**enable** | **disable**}	TCP シーケンス番号ランダム化をイネーブルまたはディセーブルにします。このキーワードは、管理クラス マップでは使用できません。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

conn-max、**embryonic-conn-max**、**per-client-embryonic-max**、および **per-client-max** の各パラメータの *n* のデフォルト値は、0（接続数の制限なし）です。

シーケンス番号ランダム化は、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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**per-client-embryonic-max** キーワードおよび **per-client-max** キーワードが追加されました。
8.0(2)	このコマンドが、セキュリティ アプライアンスへの管理トラフィックにおいて、レイヤ 3/4 管理クラス マップでも使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンド（通過トラフィック）または **class-map type management** コマンド（管理トラフィック）を使用して、タイムアウトを適用するトラフィックを定義します。次に、**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** コマンドを入力できます。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、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

（注） NAT コンフィギュレーションで最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定することもできます。両方の方法を使用して同じトラフィックにこれらの設定を行う場合は、セキュリティ アプライアンスは低い方の制限を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、セキュリティ アプライアンスはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。セキュリティ アプライアンスがクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

クライアントレス SSL 互換での管理パケットの TCP 代行受信のディセーブル化

デフォルトでは、TCP 管理接続では TCP 代行受信が常にイネーブルになっています。TCP 代行受信をイネーブルにすると、3 ウェイ TCP 接続確立のハンドシェイク パケットが代行受信されるため、セキュリティ アプライアンスではクライアントレス SSL のパケットを処理できなくなります。クライアントレス SSL では、クライアントレス SSL 接続で selective-ack や他の TCP オプションを提供するために、3 ウェイ ハンドシェイク パケットを処理する機能が必要になります。管理トラフィックの TCP 代行受信をディセーブルにするには、初期接続制限を設定します。初期接続制限に達した後にだけ TCP 代行受信をイネーブルにできます。

TCP シーケンスランダム化概要

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- セキュリティ アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

例

次に、**set connection** コマンドを使用して、同時接続最大数を 256 に設定し、TCP シーケンス番号ランダム化をディセーブルにする例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

次に、トラフィックを CSC SSM に転送するサービス ポリシーでの **set connection** コマンドの使用例を示します。**set connection** コマンドによって、CSC SSM でトラフィックがスキャンされる各クライアントが最大 5 接続に制限されます。

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

複数のパラメータを指定してこのコマンドを入力することも、各パラメータを個別のコマンドとして入力することもできます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが service-policy コマンドで使用されている場合、そのポリシー マップは削除されません。
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 policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシー設定を表示します。**set connection** コマンドを含むポリシーを表示するには、**set connection** キーワードを使用します。

set connection advanced-options

トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップ内で指定するには、クラス モードで **set connection advanced-options** コマンドを使用します。トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップから削除するには、クラス モードで、このコマンドの **no** 形式を使用します。

set connection advanced-options *tcp-mapname*

no set connection advanced-options *tcp-mapname*

構文の説明

tcp-mapname	高度な TCP 接続オプションの設定対象となる TCP マップの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行するには、TCP マップ名に加えて、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。詳細については、**tcp-map** コマンドの説明を参照してください。

例

次に、**set connection advanced-options** コマンドを使用して、localmap という名前の TCP マップの使用を指定する例を示します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
class-map	クラス マップ モードで match コマンドを 1 つだけ（tunnel-group および default-inspection-traffic を除く）発行し、一致基準を指定することによって、トラフィック クラスを設定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
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 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。

set connection decrement-ttl

ポリシー マップ内のトラフィック クラスにおいて存続可能時間の値をデクリメントするには、クラス コンフィギュレーション モードで **set connection decrement-ttl** コマンドを使用します。存続可能時間をデクリメントしない場合は、このコマンドの **no** 形式を使用します。

set connection decrement-ttl

no set connection decrement-ttl

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、セキュリティ アプライアンスでは、存続可能時間はデクリメントされません。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンド、および **icmp unreachable** コマンドは、セキュリティ アプライアンスをホップの 1 つとして表示するセキュリティ アプライアンス経由の traceroute を可能とするために必要です。

例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

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。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが **service-policy** コマンドで使用されている場合、そのポリシー マップは削除されません。
icmp unreachable	ICMP 到達不能メッセージがセキュリティ アプライアンスを通過可能なレートを制御します。

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 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。
show service-policy	サービス ポリシー設定を表示します。

set connection timeout

ポリシー マップ内のトラフィック クラスに対して接続タイムアウトを指定するには、クラス コンフィギュレーション モードで **set connection timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

構文の説明

dcd	Dead Connection Detection（DCD; デッド接続検出）をイネーブルにします。DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。TCP 接続がタイムアウトすると、セキュリティ アプライアンスは、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、セキュリティ アプライアンスはその接続を解放します。両方のエンドホストが応答して接続の有効性が確認されると、セキュリティ アプライアンスはアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。
embryonic *hh*:*mm*:*ss*	TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間を 0:0:5 ～ 1193:0:0 の範囲で設定します。デフォルトは 0:0:30 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。初期接続とは、スリーウェイ ハンドシェイクが完了していない TCP 接続です。
half-closed *hh*:*mm*:*ss*	ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間を 0:5:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 0:10:0 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。ハーフクローズの接続は DCD の影響を受けません。また、セキュリティ アプライアンスは、ハーフクローズ接続を切断するときにリセット パケットを送信しません。
max_retries	DCD において、何回連続して再試行に失敗すると接続がデッドであると見なされるかを設定します。最小値は 1、最大値は 255 です。デフォルトは 5 です。
reset	TCP のアイドル接続が削除されてから、両方のエンド システムに TCP RST パケットを送信します。
retry_interval	DCD プローブに応答がない場合に次のプローブを送信するまでの *hh*:*mm*:*ss* 形式の間隔を 0:0:1 ～ 24:0:0 の範囲で指定します。デフォルトは 0:0:15 です。
tcp *hh*:*mm*:*ss*	確立された接続が終了するアイドル タイムアウト時間を設定します。

デフォルト

デフォルトの **embryonic** タイムアウトは 30 秒です。

デフォルトの **half-closed** アイドル タイムアウトは 10 分です。

デフォルトの **dcd** *max_retries* の値は 5 です。

デフォルトの **dcd** *retry_interval* の値は 15 秒です。

デフォルトの **tcp** アイドル 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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DCD のサポートが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンドを使用して、タイムアウトを適用するトラフィックを定義します。次に、**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 timeout** コマンドを入力できます。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、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

DCD をイネーブルにすると、TCP ノーマライザでのアイドルタイムアウト処理の動作が変更されます。DCD プローブにより、**show conn** コマンドで表示される接続でのアイドル タイムアウトがリセットされます。タイムアウト コマンドで設定したタイムアウト値を超過していても、DCD プローブのために存続している接続を判別するため、**show service-policy** コマンドには、DCD からのアクティビティ数を示すカウンタが含まれています。

例

次に、すべてのトラフィックの接続タイムアウトを設定する例を示します。

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection timeout tcp 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。セキュリティ アプライアンスは、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection timeout embryonic 0:40:0
```

show running-config policy-map コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
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	接続の値を設定します。
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。
show service-policy	DCD およびその他のサービス アクティビティのカウンタを表示します。

set metric

ルーティング プロトコルのメトリック値を設定するには、ルート マップ コンフィギュレーション モードで **metric** コマンドを使用します。デフォルトのメトリック値に戻すには、このコマンドの **no** 形式を使用します。

set metric *value*

no set metric *value*

構文の説明

value	メトリック値。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

no set metric *value* コマンドを使用すると、デフォルトのメトリック値に戻すことができます。このコンテキストでは、*value* は 0 ～ 4294967295 の整数です。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

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

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
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。

set metric-type

OSPF メトリック ルートのタイプを指定するには、ルート マップ コンフィギュレーション モードで **set metric-type** 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。

set metric-type {**type-1** | **type-2**}

no set metric-type

構文の説明

type-1	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。
type-2	指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。

デフォルト

デフォルトは、**type-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。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# set metric-type type-2
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
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。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

setup

対話形式のプロンプトを使用してセキュリティ アプライアンスの最小限度のコンフィギュレー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 **setup** コマンドを入力します。このコンフィギュレーションでは、ASDM を使用するための接続が提供されます。デフォルトのコンフィギュレーションに戻すには、**configure factory-default** コマンドも参照してください。

setup

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

フラッシュ メモリにスタートアップ コンフィギュレーションがない場合は、起動時に設定ダイアログ ボックスが自動的に表示されます。

setup コマンドを使用する前に、内部インターフェイスを設定しておく必要があります。PIX 500 シリーズのデフォルト コンフィギュレーションには内部インターフェイス（イーサネット 1）が含まれていますが、ASA 550 シリーズのデフォルト コンフィギュレーションには含まれていません。**setup** コマンドを使用する前に、内部インターフェイスにするインターフェイスに対して **interface** コマンドを入力して、**nameif inside** コマンドを入力します。

マルチ コンテキスト モードでは、システム実行スペースおよび各コンテキストに対して **setup** コマンドを使用できます。

setup コマンドを入力すると、表 24-1 の情報の入力を求められます。システムの **setup** コマンドには、これらのプロンプトのサブセットが含まれています。プロンプトに表示されたパラメータのコンフィギュレーションがすでに存在する場合は、そのコンフィギュレーションが角カッコに表示されます。その値をデフォルトとして受け入れるか、または新しい値を入力してその値を上書きできます。

表 24-1　設定プロンプト

プロンプト	説明
Pre-configure Firewall now through interactive prompts [yes]?	**yes** または **no** を入力します。**yes** を入力すると、設定ダイアログボックスが続行します。**no** を入力すると、設定ダイアログボックスが停止し、グローバル コンフィギュレーション プロンプト（hostname(config)#）が表示されます。
Firewall Mode [Routed]:	**routed** または **transparent** を入力します。
Enable password:	イネーブル パスワードを入力します （パスワードは、3 文字以上である必要があります)。
Allow password recovery [yes]?	**yes** または **no** を入力します。
Clock (UTC):	このフィールドには何も入力できません。デフォルトで UTC 時間が使用されます。
Year:	4 桁の年（2005 など）を入力します。年の範囲は 1993 ～ 2035 です。
Month:	月の先頭の 3 文字（9 月の場合は **Sep** など）を使用して月を入力します。
Day:	日付（1 ～ 31）を入力します。
Time:	24 時間制で時間、分、秒を入力します。たとえば、午後 8 時 54 分 44 秒の場合は、**20:54:44** と入力します。
Inside IP address:	内部インターフェイスの IP アドレスを入力します。
Inside network mask:	内部 IP アドレスに適用するネットワーク マスクを入力します。255.0.0.0 や 255.255.0.0 などの有効なネットワーク マスクを指定する必要があります。
Host name:	コマンドライン プロンプトに表示するホスト名を入力します。
Domain name:	セキュリティ アプライアンスを稼働するネットワークのドメイン名を入力します。
IP address of host running Device Manager:	ASDM にアクセスする必要があるホストの IP アドレスを入力します。
Use this configuration and write to flash?	**yes** または **no** を入力します。**yes** を入力すると、内部インターフェイスがイネーブルになり、要求されたコンフィギュレーションがフラッシュ パーティションに書き込まれます。 **no** を入力すると、設定ダイアログボックスが最初の質問から繰り返されます。 Pre-configure Firewall now through interactive prompts [yes]? 設定ダイアログボックスを終了するには **no** を、設定ダイアログボックスを繰り返すには **yes** を入力します。

例

次に、**setup** コマンド プロンプトを完了する例を示します。

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
```

```
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

関連コマンド

コマンド	説明
configure factory-default	デフォルトのコンフィギュレーションに戻します。

shape

QoS トラフィック シェーピングをイネーブルにするには、クラス コンフィギュレーション モードで **shape** コマンドを使用します。セキュリティ アプライアンスなどの、ファスト イーサネットを使用してパケットを高速に送信するデバイスが存在し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、ケーブル モデムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされます。さまざまな回線速度を持つネットワークを管理するために、低い固定レートでパケットを送信するようにセキュリティ アプライアンスを設定できます。これを *トラフィック シェーピング*と呼びます。この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。

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

構文の説明

average *rate*	一定期間におけるトラフィックの平均レート（ビット/秒）を 64000 ～ 154400000 の範囲で設定します。8000 の倍数の値を指定します。期間の計算方法の詳細については、「使用上のガイドライン」の項を参照してください。
burst_size	一定期間において送信可能な平均バースト サイズ（ビット単位）を 2048 ～ 154400000 の範囲で設定します。128 の倍数の値を指定します。*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

デフォルト

burst_size を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 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	透過	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	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

トラフィック シェーピングをイネーブルにするには、Modular Policy Framework を使用します。

1. **policy-map**：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。

b. **shape**：トラフィック シェーピングをクラス マップに適用します。

c. （任意）**service-policy**：シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを適用できるように、**priority** コマンドを設定した異なるポリシー マップを呼び出します。

2. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

トラフィック シェーピングの概要

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延の原因になる可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。

- トラフィック シェーピングは、物理インターフェイスのすべての発信トラフィック、または ASA 5505 の場合は VLAN 上のすべての発信トラフィックに適用する必要があります。特定のタイプのトラフィックにはトラフィック シェーピングを設定できません。
- トラフィック シェーピングはインターフェイス上でパケットの送信準備が完了したときに適用されるため、レート計算は、IPSec ヘッダーや L2 ヘッダーなどのすべてのオーバーヘッドを含む、実際の送信パケット サイズに基づいて行われます。
- シェーピングされるトラフィックには、through-the-box トラフィックと from-the-box トラフィックの両方が含まれます。
- シェープ レートの計算は、標準トークン バケット アルゴリズムに基づいて行われます。トークン バケット サイズは、バースト サイズ値の 2 倍です。トークン バケットの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
- バースト性のトラフィックが指定されたシェープ レートを超えると、パケットはキューに入れられて、後で送信されます。次に、シェーピング キューのいくつかの特性について説明します（階層型プライオリティ キューイングの詳細については、**priority** コマンドを参照してください）。
  - キューのサイズは、シェープ レートに基づいて計算されます。キューは、1500 バイトのパケットとして 200 ミリ秒に相当するシェープ レート トラフィックを保持できます。最小キュー サイズは 64 です。
  - キューの制限に達すると、パケットはキューの末尾からドロップされます。
  - OSPF Hello パケットなどの一部の重要なキープアライブ パケットは、ドロップされません。
  - 時間間隔は、*time_interval* = *burst_size* / *average_rate* によって求められます。時間間隔が長くなるほど、シェープ トラフィックのバースト性は高くなり、リンクのアイドル状態が長くなる可能性があります。この効果は、次のような誇張した例を使うとよく理解できます。

    平均レート = 1000000

    バースト サイズ = 1000000

    この例では、時間間隔は 1 秒であり、これは、100 Mbps の FE リンクでは 1 Mbps のトラフィックを時間間隔 1 秒の最初の 10 ミリ秒内にバースト送信できることを意味し、残りの 990 ミリ秒間はアイドル状態になって、次の時間間隔になるまでパケットを送信できません。したがって、音声トラフィックのように遅延が問題になるトラフィックがある場合は、バースト サイズを平均レートと比較して小さくし、時間間隔を短くする必要があります。

QoS 機能の相互作用のしくみ

セキュリティ アプライアンスで必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能をセキュリティ アプライアンスに設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。たとえば、グローバル ポリシーに標準プライオリティ キューイングを設定して、特定のインターフェイスにトラフィック シェーピングを設定する場合、最後に設定した機能は拒否されます。これは、グローバル ポリシーがインターフェイス ポリシーと重複するためです。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定はセキュリティ アプライアンスでは制限されていません。

例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップ内でアクションを実行するクラス マップを指定します。
police	QoS ポリシングをイネーブルにします。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
priority	QoS プライオリティ キューイングをイネーブルにします。
service-policy（クラス）	階層型ポリシー マップを適用します。
service-policy（グローバル）	サービス ポリシーをインターフェイスに適用します。
show service-policy	QoS 統計情報を表示します。

show aaa local user

現在ロックされているユーザ名のリストを表示するか、またはユーザ名の詳細を表示するには、グローバル コンフィギュレーション モードで **aaa local user** コマンドを使用します。

show aaa local user [locked]

構文の説明

locked	（任意）現在ロックされているユーザ名のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションのキーワード **locked** を省略すると、セキュリティ アプライアンスによって、すべての AAA ローカル ユーザの失敗試行およびロックアウト ステータスの詳細が表示されます。

username オプションを使用して単一のユーザを指定するか、**all** オプションを使用してすべてのユーザを指定できます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響します。

管理者をデバイスからロックアウトすることはできません。

例

次に、**show aaa local user** コマンドを使用して、すべてのユーザ名のロックアウト ステータスを表示する例を示します。

次に、制限を 5 回に設定した後に **show aaa local user** コマンドを使用して、すべての AAA ローカル ユーザの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

次に、制限を 5 回に設定した後に **lockout** キーワードを指定して **show aaa local user** コマンドを使用し、ロックアウトされている AAA ローカル ユーザのみの失敗した認証試行回数およびロックアウト ステータスの詳細を表示する例を示します。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザが何回誤ったパスワードを入力するとロック アウトされるかを示す最大回数を設定します。
clear aaa local user fail-attempts	ロックアウト ステータスを変更しないで、失敗試行回数を 0 にリセットします。
clear aaa local user lockout	指定したユーザまたはすべてのユーザのロックアウト ステータスをクリアして、それらのユーザの失敗試行カウンタを 0 に設定します。

show aaa-server

AAA サーバの AAA サーバ統計情報を表示するには、特権 EXEC モードで **show aaa-server** コマンドを使用します。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

LOCAL	（任意）ローカル ユーザ データベースの統計情報を表示します。
groupname	（任意）グループ内のサーバの統計情報を表示します。
host *hostname*	（任意）グループ内の特定のサーバの統計情報を表示します。
protocol *protocol*	（任意）指定したプロトコルのサーバの統計情報を表示します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトで、すべての AAA サーバ統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	http-form プロトコルが追加されました。
8.0(2)	**aaa-server active** コマンドまたは **fail** コマンドを使用して手動でステータスが変更されたかどうかがサーバ ステータスに表示されるようになりました。

例

次に、**show aaa-server** コマンドを使用して、サーバ グループ group1 の特定のホストの統計情報を表示する例を示します。

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
```

```
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

次に、**show aaa-server** コマンドのフィールド説明を示します。

フィールド	説明
Server Group	**aaa-server** コマンドによって指定されたサーバ グループ名。
Server Protocol	**aaa-server** コマンドによって指定されたサーバ グループのサーバ プロトコル。
Server Address	AAA サーバの IP アドレス。
Server port	セキュリティ アプライアンスおよび AAA サーバによって使用される通信ポート。RADIUS 認証ポートは、**authentication-port** コマンドを使用して指定できます。RADIUS アカウンティング ポートは、**accounting-port** コマンドを使用して指定できます。非 RADIUS サーバでは、ポートは **server-port** コマンドによって設定されます。
Server status	サーバのステータス。次のいずれかの値が表示されます。 • ACTIVE : セキュリティ アプライアンスはこの AAA サーバと通信します。 • FAILED : セキュリティ アプライアンスはこの AAA サーバと通信できません。この状態になったサーバは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。 ステータスの後に「(admin initiated)」と表示されている場合、このサーバは、**aaa-server active** コマンドまたは **fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。 また、次の形式で最終トランザクションの日時も表示されます。 **Last transaction ({success | failure}) at** *time timezone date* セキュリティ アプライアンスがサーバと通信したことがない場合は、次のメッセージが表示されます。 **Last transaction at Unknown**
Number of pending requests	現在進行中の要求数。
Average round trip time	サーバとのトランザクションを完了するまでにかかる平均時間。
Number of authentication requests	セキュリティ アプライアンスによって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。

フィールド	説明
Number of authorization requests	認可要求数。この値は、コマンド認可、through-the-box トラフィックの認可（TACACS+ サーバ）、またはトンネル グループに対してイネーブルにされた WebVPN および IPSec 認可機能による認可要求を指しています。この値には、タイムアウト後の再送信は含まれていません。
Number of accounting requests	アカウンティング要求数。この値には、タイムアウト後の再送信は含まれていません。
Number of retransmissions	内部タイムアウト後にメッセージが再送信された回数。この値は、Kerberos および RADIUS サーバ（UDP）にのみ適用されます。
Number of accepts	成功した認証要求数。
Number of rejects	拒否された要求数。この値には、エラー状態、および実際にクレデンシャルが AAA サーバから拒否された場合の両方が含まれます。
Number of challenges	最初にユーザ名とパスワードの情報を受信した後に、AAA サーバがユーザに対して追加の情報を要求した回数。
Number of malformed responses	該当なし。将来的な使用のために予約されています。
Number of bad authenticators	次のいずれかが発生した回数。 • RADIUS パケットの「authenticator」ストリングが破損している（まれなケース）。 • セキュリティ アプライアンスの共有秘密キーと RADIUS サーバの共有秘密キーが一致しない。この問題を修正するには、適切なサーバ キーを入力します。 この値は、RADIUS にのみ適用されます。
Number of timeouts	セキュリティ アプライアンスが、AAA サーバが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。
Number of unrecognized responses	認識できない応答またはサポートしていない応答をセキュリティ アプライアンスが AAA サーバから受信した回数。たとえば、サーバからの RADIUS パケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」、または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバからの RADIUS 応答パケットが破損していることを意味していますが、まれなケースです。

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバ グループ内のすべてのサーバ、または特定のサーバの統計情報を表示します。
clear aaa-server statistics	AAA サーバ統計情報をクリアします。

show access-list

アクセス リストのカウンタを表示するには、特権 EXEC モードで **show access-list** コマンドを使用します。

show access-list *id_1* [...[*id_2*]] [**brief**]

構文の説明

acl_name_1	既存のアクセス リストを識別する名前または文字セット。
acl_name_2	既存のアクセス リストを識別する名前または文字セット。
brief	アクセス リスト識別子およびヒット カウントを 16 進数形式で表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	**brief** キーワ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

1 つのコマンドに複数のアクセス リスト識別子を入力することによって、一度に複数のアクセス リストを表示できます。

brief キーワードを指定して、16 進数形式でアクセス リスト ヒット カウントおよび識別子情報を表示できます。16 進数形式で表示されるコンフィギュレーション識別子は 2 列に表示され、syslog 106023 および 106100 で使用される識別子と同じです。

例

次に、**show access-list** コマンドの出力例を示します。

```
hostname# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 10 elements
access-list 101 line 1 extended permit tcp any eq www any (hitcnt=0) 0xa14fc533
access-list 101 line 2 extended permit tcp any eq www any eq www (hitcnt=0) 0xaa73834e
access-list 101 line 3 extended permit tcp any eq www any range telnet www (hitcnt=0)
0x49ac02e6
access-list 101 line 4 extended permit tcp any range telnet www any range telnet www
(hitcnt=0) 0xa0021a9f
access-list 101 line 5 extended permit udp any range biff www any (hitcnt=0) 0xf89a7328
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43 access-list
101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
```

```
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

この出力では、各行の最後に個々のアクセス コントロール エントリに対する独自の 16 進数の識別子が含まれています。

次に、**show access-list brief** コマンドの出力例を示します。

```
hostname (config)# sh access-list abc brief

abc:
28676dfa 00000000 00000001
bbec063f f0109e02 000000a1
3afd0576 f0109e02 000000c2
a83ddc02 f0109e02 00000021
hostname (config)#
```

最初の 2 列に識別子が 16 進数形式で表示され、3 列めにヒット カウントが 16 進数形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。ヒット カウントがゼロの場合、情報は表示されません。

関連コマンド

コマンド	説明
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show activation-key

実行アクティベーション キー、および許可されているコンテキスト数を含む、アクティベーション キーによってイネーブルにされているコンフィギュレーション内のライセンス済み機能を表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。

show activation-key [detail]

（注）　このコマンドは、PIX プラットフォームではサポートされません。

構文の説明

detail キーワードを使用すると、永久アクティベーション キーと一時アクティベーション キーおよびこれらのキーによってイネーブルにされる機能が表示されます（以前にインストールされたすべての一時キーおよびこれらのキーの有効期限を含む）。

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。

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

コマンド履歴

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

使用上のガイドライン

show activation-key コマンド出力では、次のようにアクティベーション キーのステータスが表示されます。

- セキュリティ アプライアンス のフラッシュ ファイル システム内のアクティベーション キーがセキュリティ アプライアンスで実行されているアクティベーション キーと同じである場合、**show activation-key** の出力は次のようになります。

```
The flash activation key is the SAME as the running key.
```

- セキュリティ アプライアンス のフラッシュ ファイル システムのアクティベーション キーとセキュリティ アプライアンスで稼働するアクティベーション キーが異なる場合、**show activation-key** の出力は次のようになります。

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- アクティベーション キーをダウングレードすると、動作中のキー（古いキー）とフラッシュに格納されているキー（新しいキー）が異なることを示す出力が表示されます。セキュリティ アプライアンス を再起動すると、新しいキーが使用されます。
- アクティベーション キーをアップグレードして、追加の機能をイネーブルにした場合は、再起動しなくても新しいキーがただちに動作を開始します。
- PIX Firewall プラットフォームでは、新しいキーと古いキーの間でフェールオーバー機能（R/UR/FO）に変更があった場合、確認が求められます。**n** を入力すると、変更が中止されます。それ以外の場合は、フラッシュ ファイル システムのキーが更新されます。セキュリティ アプライアンス を再起動すると、新しいキーが使用されます。
- 以前のリリースにダウングレードした場合、現在のリリースのキーでは、以前のリリースでサポートされている数よりも多くのセキュリティ コンテキストが使用できる場合があります。キーのセキュリティ コンテキストの値がプラットフォームの制限を超えると、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: 50 security contexts exceeds the limit in the
  platform, reduce to 20 security contexts.
  ```

- 以前のリリースにダウングレードした場合、現在のリリースのキーでは GTP/GPRS がイネーブルであるにもかかわらず、以前のリリースでは GTP/GPRS が許可されていないことがあります。キーを使用して GTP/GPRS をイネーブルにしても、GTP/GPRS がソフトウェアのバージョンによって許可されない場合は、show activation-key の出力に次のメッセージが表示されます。

  ```
  The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
  GTP/GPRS.
  ```

一時アクティベーション キーは時間ベースのアクティベーション キーであり、このキーは、**activation-key** コマンドを使用して有効または無効にできます。一時アクティベーション キーを無効にすると、永久アクティベーション キーを割り当てることができます。永久アクティベーション キーは、非時間ベースのアクティベーション キーです。一時アクティベーション キーは、後で再度アクティブにできるので削除できません。

一時アクティベーション キーと永久アクティベーション キーは、両方ともフラッシュ ファイル システムに保管されます。適用されるキーは、機能しているアクティベーション キーです。一時アクティベーション キーは、一度に 1 つだけ適用できます。一時アクティベーション キーがすでに適用されているセキュリティ アプライアンスに一時アクティベーション キーを適用すると、古い一時アクティベーション キーは無効になり、新しい一時アクティベーション キーが適用されます。

セキュリティ アプライアンスは、アクティブになっているすべての一時アクティベーション キーを追跡します。一時アクティベーション キーが失効すると、セキュリティ アプライアンスにより、失効したことが通知されます。一時アクティベーション キーは、失効すると表示されなくなります。アクティブでない一時アクティベーション キーは、別の一時アクティベーション キーまたは永久アクティベーション キーによって適用され、上書きされたキーです。

例

次に、コンフィギュレーション内のコマンドのうち、アクティベーション キーでイネーブルにされた機能に関するものを表示する例を示します。

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada
The Running Activation Key feature: 50 security contexts exceeds the limit in the
platform, reduce to 20 security contexts.
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
GTP/GPRS.

License Features for this Platform:
Maximum Physical Interfaces : Unlimited
```

```
Maximum VLANs               : 50
Inside Hosts                : Unlimited
Failover                    : Enabled
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL-filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
VPN Peers                   : 5000
Advanced Endpoint Assessment: Disabled
UC Proxy Sessions            : 2

The flash activation key is the SAME as the running key.
```

次の例は、一時アクティベーション キーおよび永久アクティベーション キーによってイネーブルになったコンフィギュレーションに含まれているライセンス付き機能を表示する方法を示しています。

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
Permanent Flash Activation Key: 0x31245147 0x3834b49a 0x98b391b4
0x95b83030 0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

Temporary Flash Activation Key: 0x051e96ff 0x98937617 0x79cbe717
0x502449e7 0x862b92ab

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Disabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
WebVPN Peers                 : 2
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions            : 2
This is a time-based license that will expire in 27 day(s).
```

次の例は、永久アクティベーション キーによってイネーブルになったコンフィギュレーションに含まれているライセンス付き機能を表示する方法を示しています。

```
hostname(config)# show activation-key detail
```

```
Serial Number:  JMX0916L0Z4
No active temporary key.
Running Activation Key: 0x31245147 0x3834b49a 0x98b391b4 0x95b83030
0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

This platform has an ASA 5540 VPN Premium license.

The flash activation key is the SAME as the running key.

Non-active temporary keys:                                Time left
-----------------------------------------------------------------------
0x2a53d6   0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2  28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397  27 day(s
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを変更します。

show ad-groups

Active Directory サーバにリストされているグループを表示するには、特権 EXEC モードで **show ad-groups** コマンドを使用します。

show ad-groups *name* [**filter** *string*]

構文の説明

name	問い合わせる Active Directory サーバ グループの名前。
string	検索するグループ名の全体または一部を指定する、引用符で囲んだ問い合わせに含めるストリング。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

show ad-groups コマンドは、グループの取得に LDAP プロトコルを使用する Active Directory サーバに対してのみ適用されます。このコマンドを使用して、ダイナミック アクセス ポリシー AAA 選択基準に使用できる AD グループを表示します。

LDAP 属性タイプが LDAP の場合、セキュリティ アプライアンスがサーバからの応答を待機するデフォルト時間は 10 秒です。この時間は、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用して調整できます。

（注） Active Directory サーバに数多くのグループが含まれている場合は、サーバが応答パケットに格納できるデータ量の制限に基づいて **show ad-groups** コマンドの出力が切り捨てられることがあります。この問題を回避するには、**filter** オプションを使用して、サーバからレポートされるグループ数を減らします。

例

```
hostname# show ad-groups LDAP-AD17
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

次に、同じコマンドで **filter** オプションを使用した例を示します。

```
hostname(config)# show ad-groups LDAP-AD17 filter "Eng"
.
Server Group    LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups       4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
group-search-timeout	グループのリストについて Active Directory サーバからの応答をセキュリティ アプライアンスが待機する時間を調整します。

show admin-context

現在管理コンテキストとして割り当てられているコンテキスト名を表示するには、特権 EXEC モードで **show admin-context** コマンドを使用します。

show admin-context

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show admin-context** コマンドの出力例を示します。次の例では、「admin」という名前で、フラッシュのルート ディレクトリに保存されている管理コンテキストが表示されています。

```
hostname# show admin-context
Admin: admin flash:/admin.cfg
```

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。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
clear configure context	すべてのコンテキストを削除します。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

show arp

ARP テーブルを表示するには、特権 EXEC モードで **show arp** コマンドを使用します。

show arp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	表示にダイナミック ARP エージングが追加されました。

使用上のガイドライン

表示出力には、ダイナミック、スタティック、およびプロキシ ARP エントリが表示されます。ダイナミック ARP エントリには、ARP エントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARP エントリにはダッシュ（-）が、プロキシ ARP エントリには「alias」という状態が含まれています。

例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
hostname# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、特権 EXEC モードで **show arp-inspection** コマンドを使用します。

show arp-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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show arp-inspection** コマンドの出力例を示します。

```
hostname# show arp-inspection
interface                arp-inspection         miss
-------------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp statistics

ARP 統計情報を表示するには、特権 EXEC モードで show arp statistics コマンドを使用します。

show arp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show arp statistics** コマンドの出力例を示します。

```
hostname# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 2 に、各フィールドの説明を示します。

表 24-2　show arp statistics のフィールド

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。
Maximum queued blocks	IP アドレスの解決を待機している間に ARP モジュールにキューイングされた最大ブロック数。
Queued blocks	現在 ARP モジュールにキューイングされているブロック数。

表 24-2　show arp statistics のフィールド （続き）

フィールド	説明
Interface collision ARPs received	セキュリティ アプライアンスのインターフェイスと同じ IP アドレスからの ARP パケットがセキュリティ アプライアンスのすべてのインターフェイスで受信されたパケット数。
ARP-defense gratuitous ARPs sent	ARP-Defense メカニズムの一環としてセキュリティ アプライアンスによって送信された Gratuitous ARP の数。
Total ARP retries	最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。
Unresolved hosts	現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。
Maximum unresolved hosts	最後にクリアされた後、またはセキュリティ アプライアンスの起動後に、ARP モジュールに存在した未解決ホストの最大数。

関連コマンド

コマンド	説明
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報をクリアして、値をゼロにリセットします。
show arp	ARP テーブルを表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show asdm history

ASDM 履歴バッファの内容を表示するには、特権 EXEC モードで **show asdm history** コマンドを使用します。

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

構文の説明

asdmclient	（任意）ASDM クライアント用にフォーマットされた ASDM 履歴データを表示します。
feature *feature*	（任意）履歴表示を指定した機能に制限します。*feature* 引数には、次の値を指定できます。 • **all**：すべての機能の履歴を表示します（デフォルト）。 • **blocks**：システム バッファの履歴を表示します。 • **cpu**：CPU 使用状況の履歴を表示します。 • **failover**：フェールオーバーの履歴を表示します。 • **ids**：IDS の履歴を表示します。 • **interface** *if_name*：指定したインターフェイスの履歴を表示します。*if_name* 引数は、**nameif** コマンドで指定したインターフェイスの名前です。 • **memory**：メモリ使用状況の履歴を表示します。 • **perfmon**：パフォーマンス履歴を表示します。 • **sas**：セキュリティ アソシエーションの履歴を表示します。 • **tunnels**：トンネルの履歴を表示します。 • **xlates**：変換スロット履歴を表示します。
snapshot	（任意）最後の ASDM 履歴データ ポイントのみを表示します。
view *timeframe*	（任意）履歴の表示を指定した期間に制限します。*timeframe* 引数には、次の値を指定できます。 • **all**：履歴バッファ内のすべての内容（デフォルト）。 • **12h**：12 時間 • **5d**：5 日 • **60m**：60 分 • **10m**：10 分

デフォルト

引数またはキーワードを指定しない場合は、すべての機能のすべての履歴情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm history** コマンドから **show asdm history** コマンドに変更されました。

使用上のガイドライン

show asdm history コマンドは、ASDM 履歴バッファの内容を表示します。ASDM 履歴情報を表示する前に、**asdm history enable** コマンドを使用して、ASDM 履歴トラッキングをイネーブルにする必要があります。

例

次に、**show asdm history** コマンドの出力例を示します。このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。

```
hostname# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
```

```
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

次に、**show asdm history** コマンドの出力例を示します。前の例と同様に、このコマンドでは、直近の 10 分間に収集された外部インターフェイスのデータに出力が制限されています。ただし、この例では、出力は ASDM クライアント用にフォーマットされています。

```
hostname# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|
25026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|
25102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|
25169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|
25381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750|
750|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|751|751|
751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753|753|
753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|55|
55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|
55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|
4381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|
5401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698|
5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349|
5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|3349|
5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|
5|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|
7|6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
```

```
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|
375010|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|
375395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|
375794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|
376200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|
128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
hostname#
```

次に、**snapshot** キーワードを使用した **show asdm history** コマンドの出力例を示します。

```
hostname# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
```

```
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
```

```
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
```

```
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
hostname#
```

関連コマンド

コマンド	説明
asdm history enable	ASDM 履歴トラッキングをイネーブルにします。

show asdm image

現在の ASDM ソフトウェア イメージ ファイルを表示するには、特権 EXEC モードで **show asdm image** コマンドを使用します。

show asdm image

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm image** コマンドから **show asdm image** コマンドに変更されました。

例

次に、**show asdm image** コマンドの出力例を示します。

```
hostname# show asdm image

Device Manager image file, flash:/ASDM
```

関連コマンド

コマンド	説明
asdm image	現在の ASDM イメージ ファイルを指定します。

show asdm log_sessions

アクティブな ASDM ロギング セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm log_sessions** コマンドを使用します。

show asdm log_sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから Syslog メッセージを取得します。各 ASDM ロギング セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect log_session** コマンドで使用して、指定したセッションを終了できます。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギング セッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

例

次に、**show asdm log_sessions** コマンドの出力例を示します。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect log_session	アクティブな ASDM ロギング セッションを終了します。

show asdm sessions

アクティブな ASDM セッション、およびそれらに関連するセッション ID のリストを表示するには、特権 EXEC モードで **show asdm sessions** コマンドを使用します。

show asdm sessions

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm sessions** コマンドから **show asdm sessions** コマンドに変更されました。

使用上のガイドライン

アクティブな各 ASDM セッションには、一意のセッション ID が割り当てられます。このセッション ID を **asdm disconnect** コマンドで使用して、指定したセッションを終了できます。

例

次に、**show asdm sessions** コマンドの出力例を示します。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect	アクティブな ASDM セッションを終了します。