CHAPTER 24

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

same-security-traffic

セキュリティ レベルが等しいインターフェイス間での通信を許可する、またはトラフィックが同じインターフェイスへ入る、または出るのを許可するには、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。セキュリティの等しいトラフィック間での通信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**}

シンタックスの説明

inter-interface	セキュリティ レベルの等しい複数の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の通信のインおよびアウトを許可します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、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
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)(1)	このコマンドが導入されました。
7.2(1)	このバージョン以降は、**intra-interface** キーワードを使用すると、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出入りできます。

使用上のガイドライン

セキュリティ レベルが等しいインターフェイス間での通信を許可（**same-security-traffic inter-interface** コマンドを使用）すると、次の利点があります。

- 101 個を超える通信インターフェイスを設定できる。インターフェイスごとにそれぞれ別のレベルを使用する場合、設定できるインターフェイスは各レベル（0 ～ 100）に 1 つのみです。
- セキュリティ レベルの等しいすべてのインターフェイス間で、アクセス リストとは無関係に、トラフィックを自由に送受信できる。

same-security-traffic intra-interface コマンドを使用すると、通常は許可されていない、トラフィックによる同一インターフェイスへの出入りが可能になります。この機能は、あるインターフェイスに入り、同じインターフェイスから出る VPN トラフィックに役立ちます。この場合、VPN トラフィックの暗号化は解除されるか、別の VPN 接続に対して再暗号化されます。たとえば、ハブまたはスポークの VPN ネットワークがあるとします。セキュリティ アプライアンスがハブで、リモート VPN ネットワークがスポークであり、一方のスポークが別のスポークと通信する場合、トラフィックはセキュリティ アプライアンスに入り、その後別のスポークに向けて出て行かなければなりません。

例

次の例は、セキュリティ レベルの等しいインターフェイス間での通信をイネーブルにする方法を示しています。

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

次の例では、トラフィックが同じインターフェイスに入り、出て来るようにする方法を示します。

```
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** のコンフィギュレーションを表示します。

sasl-mechanism

LDAP サーバに対する LDAP クライアントの認証に SASL（Simple Authentication and Security Layer）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 ユーザにとってセキュリティ アプライアンスは、LDAP サーバに対するクライアント プロキシとして機能するため、ここでいう LDAP クライアントとは、セキュリティ アプライアンスのことです。

シンタックスの説明

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 の値で応答します。
kerberos	セキュリティ アプライアンスは、GSSAPI（Generic Security Services Application Programming Interface）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で応答します。
server-group-name	Kerberos AAA サーバ グループを指定します（最大 64 文字）。

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形式で 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 で LDAP 通信を保護することをお勧めします。

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
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

このコマンドを使用して、LDAP サーバに対するセキュリティ アプライアンスの認証に SASL メカニズムを使用するよう指定します。

セキュリティ アプライアンスも LDAP サーバも、複数の SASL 認証メカニズムをサポートできます。SASL 認証のネゴシエート時には、セキュリティ アプライアンスはサーバ上に設定されている SASL メカニズムのリストを取得し、セキュリティ アプライアンスとサーバの両方で設定されている最も強固なメカニズムとして SASL 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固です。たとえば、LDAP サーバもセキュリティ アプライアンスも両方のメカニズムをサポートしている場合、セキュリティ アプライアンスはより強固なメカニズムである Kerberos を選択します。

SASL メカニズムをディセーブルにする場合、これらのメカニズムは個別に設定されるため、ディセーブルにするメカニズムごとに **no** コマンドを入力する必要があります。明確にディセーブルにしないと、メカニズムは有効になったままです。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、次のコマンドを両方とも入力する必要があります。

no sasl-mechanism digest-md5

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

例

次の例は、AAA サーバ ホスト コンフィギュレーション モードに入り、IP アドレスが 10.10.0.1 で ldapsvr1 という名前の LDAP サーバに対する認証として、SASL メカニズムをイネーブルにしています。この例は、SASL digest-md5 認証メカニズムをイネーブルにしています。

```
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)# sasl-mechanism digest-md5
hostname(config-aaa-server-host)#
```

次の例は、SASL Kerberos 認証メカニズムをイネーブルにし、Kerberos AAA サーバとして kerb-servr1 を指定しています。

```
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)# sasl-mechanism kerberos kerbsvr1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL によって LDAP クライアントとサーバの接続を保護するよう指定します。
server-type	LDAP サーバのベンダーを Microsoft または Sun として指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

secondary

フェールオーバー グループ内のセカンダリ装置に高い優先順位を与えるには、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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

secondary

no secondary

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバー グループに対して **primary** または **secondary** を指定しない場合、そのフェールオーバー グループは、デフォルトでは **primary** に設定されます。

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
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の優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちら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、優先する装置が使用可能になったときにその装置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	優先する装置が使用可能になったときに、フェールオーバー グループをその装置上で強制的にアクティブにします。
primary	プライマリ装置に対して、セカンダリ装置よりも高い優先順位を与えます。

secondary-color

WebVPN のログイン ページ、ホーム ページ、およびファイル アクセス ページに 2 番目の色を設定するには、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

シンタックスの説明

color	（オプション）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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。 • HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。 • 名前の長さは、最大で 32 文字です。

デフォルト

デフォルトの 2 番目の色は、HTML の #CCCCFF（薄紫色）です。

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
Webvpn	•	•	—	—	•

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

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、その中の 40 色は、Macintosh と PC では別の色が表示されます。最適な表示結果を得るには、各所で公開されている RGB テーブルを確認してください。RGB テーブルをオンラインで見つけるには、検索エンジンで RGB と入力します。

例

次の例は、HTML 色値 #5F9EAO（灰青色）を設定する方法を示しています。

```
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 タイトルバーに色を設定します。

secondary-text-color

WebVPN のログイン ページ、ホーム ページ、およびファイル アクセス ページでテキストの 2 番目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

シンタックスの説明

auto	text-color コマンドの設定に基づいて黒または白を選択します。つまり、最初の色が黒の場合、この値は白となります。
black	デフォルトのテキストの 2 番目の色は黒です。
white	テキストの色を白に変更できます。

デフォルト

デフォルトのテキストの 2 番目の色は黒です。

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
Webvpn	•	—	•	—	—

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

次の例では、テキストの 2 番目の色を白に設定する方法を示します。

```
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に色を設定します。

secure-unit-authentication

Secure Unit Authentication（SUA）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。Secure Unit Authentication 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。Secure Unit Authentication アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、Secure Unit Authentication の値を別のグループ ポリシーから継承できます。

Secure Unit Authentication 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、ユーザ名とパスワードを使用して認証を受けるように要求して、セキュリティを強化します。この機能がイネーブルになっている場合、ハードウェア クライアントは保存されているユーザ名とパスワードを使用できません。

（注） この機能がイネーブルになっているときに VPN トンネルを確立するには、ユーザ名とパスワードを入力するユーザがいる必要があります。

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

no secure-unit-authentication

シンタックスの説明

disable	Secure Unit Authentication をディセーブルにします。
enable	Secure Unit Authentication をイネーブルにします。

デフォルト

Secure Unit Authentication はディセーブルです。

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
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

Secure Unit Authentication を使用するには、ハードウェア クライアントの使用するトンネル グループ用に認証サーバグループを設定しておく必要があります。

プライマリ セキュリティ アプライアンス上で Secure Unit Authentication を要求する場合は、すべてのバックアップ サーバ上でも認証サーバグループを設定する必要があります。

例

次の例は、Secure Unit Authentication を FirstGroup というグループ ポリシーに対してイネーブルにする方法を示しています。

```
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	ユーザ認証を受けずに IP 電話を接続できるようにします。Secure Unit Authentication は有効なままになります。
leap-bypass	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（有効になっている場合）前に VPN トンネルを通過することを許可します。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。
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 レベルとは、2 つのネットワーク間に保護手段を追加して、セキュリティの高いネットワークをセキュリティの低いネットワークから保護するものです。

security-level *number*

no security-level

シンタックスの説明

number	0（最低）～ 100（最高）の整数。

デフォルト

デフォルトでは、セキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を付けて、セキュリティ レベルを明示的に設定しなかった場合、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します（**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
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

セキュリティ 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：デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのアクセス（発信）は暗黙的に許可されます。セキュリティの高いインターフェイス上にあるホストは、セキュリティの低いインターフェイス上にあるすべてのホストにアクセスできます。アクセスを制限するには、インターフェイスにアクセス リストを適用します。

  セキュリティ レベルの等しいインターフェイスが複数ある場合、セキュリティ レベルが同等またはそれ以下である他のインターフェイスへのアクセスは、暗黙的に許可されます。
- 検査エンジン：一部の検査エンジンは、セキュリティ レベルに依存します。セキュリティ レベルの等しいインターフェイスが複数ある場合、検査エンジンは双方向のトラフィックに適用されます。
  - NetBIOS 検査エンジン：発信接続にのみ適用されます。
  - OraServ 検査エンジン：2 つのホスト間で OraServ ポートの制御接続が存在する場合、セキュリティ アプライアンスでは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）と FTP のフィルタリングは、（高レベルから低レベルへの）発信接続にのみ適用されます。

  セキュリティ レベルの等しいインターフェイスが複数ある場合は、双方向のトラフィックをフィルタリングできます。

- NAT 制御：NAT 制御をイネーブルにする場合、セキュリティの高いインターフェイス（内部）上にあるホストがセキュリティの低いインターフェイス（外部）上にあるホストにアクセスする場合は、セキュリティの高いインターフェイス上にあるホストに対して NAT を設定する必要があります。

  NAT 制御を使用しない場合や、セキュリティ レベルの等しい複数のインターフェイス間では、任意のインターフェイス間に NAT を使用することも、NAT を使用しないこともできます。外部インターフェイスに対して NAT を設定する場合は、特殊なキーワードが必要になることがあります。

- **established** コマンド：このコマンドは、セキュリティ レベルの高いホストから低いホストに向かう接続がすでに確立されている場合に、セキュリティの低いホストからセキュリティの高いホストへのリターン接続を許可します。

  セキュリティ レベルの等しいインターフェイスが複数ある場合は、双方向に対して **established** コマンドを設定できます。

通常、セキュリティ レベルの等しいインターフェイス間では通信できません。セキュリティ レベルの等しいインターフェイス間で通信する必要がある場合は、**same-security-traffic** コマンドを参照してください。101 個を超える通信インターフェイスを作成する場合や、2 つのインターフェイス間で発生するトラフィックに対して同等に保護機能を適用する場合は、2 つのインターフェイスに同じセキュリティ レベルを割り当てて、通信を許可することがあります。たとえば、同等のセキュリティを必要とする 2 つの部署がある場合などです。

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には、**clear local-host** コマンドを使用して接続を消去します。

例

次の例では、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 に設定しています。

```
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 モードに入ります。
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 Accounting-Response Start および Stop メッセージを RADIUS Accounting-Request Start および Stop メッセージの送信者に送信するには、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できます。

このオプションは、デフォルトではディセーブルになっています。

send response

no send response

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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

次の例では、RADIUS アカウンティングを指定した応答を送信する方法を示します。

```
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検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

serial-number

セキュリティ アプライアンスのシリアル番号を登録時に証明書に含めるには、暗号 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、シリアル番号を含めない設定になっています。

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
暗号 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(1)	このコマンドが導入されました。

例

次の例では、central というトラストポイントの暗号 CA トラストポイント コンフィギュレーション モードに入って、セキュリティ アプライアンスのシリアル番号をトラストポイント central の登録要求に含めています。

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

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

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、適切な電子メールプロキシ モードで **server** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。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すると、要求をデフォルト電子メール サーバに送信します。デフォルト サーバを設定しない場合、ユーザもサーバを指定しなかったときは、セキュリティ アプライアンスはエラーを返します。

server {*ipaddr or hostname*}

no server

シンタックスの説明

hostname	デフォルト電子メールプロキシ サーバの DNS 名。
ipaddr	デフォルト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
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

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

次の例は、デフォルト POP3S 電子メール サーバの IP アドレスを 10.1.1.7 に設定する方法を示しています。

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

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。指定したサーバ 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

シンタックスの説明

port-number	0 ～ 65535 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
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

次の例では、「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しています。

```
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
hostname(config-aaa-server-host)#
```

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 サーバ名と VPN サーバ名のデリミタとなる文字を指定するには、適切な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。デフォルトのコロン（:）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

シンタックスの説明

symbol	電子メール サーバ名と VPN サーバ名を区切る文字。使用できるのは、アットマーク（@）、パイプ（|）、コロン（:）、番号記号（#）、カンマ（,）、およびセミコロン（;）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
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

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

サーバ セパレータは、名前セパレータとは別の文字にする必要があります。

例

次の例は、パイプ（|）を IMAP4S のサーバ セパレータとして設定する方法を示しています。

```
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、パスワードを区切る文字を指定します。

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 アプライアンスは次のサーバ モデルをサポートしています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前は Sun ONE Directory Server と呼ばれていた）

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**}

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

シンタックスの説明

auto-detect	セキュリティ アプライアンスが自動検出によって LDAP サーバ タイプを決定するように指定します。
microsoft	LDAP サーバが Microsoft Active Directory 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、自動検出によりサーバ タイプを決定するようになっています。

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
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 アプライアンスは LDAP バージョン 3 をサポートし、Sun Microsystems JAVA System Directory Server および Microsoft Active Directory のみと互換性があります。

（注）

- Sun：Sun のディレクトリ サーバにアクセスするためにセキュリティ アプライアンスで設定された DN は、そのサーバのデフォルト パスワード ポリシーにアクセスできなければなりません。DN としてディレクトリ管理者か、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 を置くことができます。
- Microsoft：Microsoft Active Directory を使用してパスワードを管理できるように、SSL で LDAP を設定する必要があります。

デフォルトでは、セキュリティ アプライアンスは、接続先が Microsoft または Sun の LDAP ディレクトリ サーバであるかどうかを自動検出します。ただし、自動検出による LDAP サーバ タイプの決定が失敗した場合でも、LDAP サーバが Microsoft または Sun のどちらであるかがわかっている場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバに手動で設定できます。

例

次の例では、AAA サーバ ホスト コンフィギュレーション モードに入り、サーバ タイプを IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 に設定します。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
hostname(config-aaa-server-host)#
```

次の例では、セキュリティ アプライアンスが自動検出によってサーバ タイプを決定するように指定しています。

```
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 auto-detect
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL によって LDAP クライアントとサーバの接続を保護するよう指定します。
sasl-mechanism	LDAP クライアントとサーバ間の 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）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

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**}

シンタックスの説明

interface *interface_name*	指定され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 アプライアンスを通過しようとしたが、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスに拒否されたすべての着信 TCP セッションの TCP リセットを送信します。セキュリティ レベルが同じインターフェイス間のトラフィックにも影響します。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。インターフェイスが指定されていない場合、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 アプライアンスを通過しようとしたが、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスに拒否されたすべての発信 TCP セッションの TCP リセットを送信します。セキュリティ レベルが同じインターフェイス間のトラフィックにも影響します。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。このオプションは、デフォルトではイネーブルになっています。たとえば、トラフィック ストームなどで CPU の負荷を軽減するために、発信リセットをディセーブルにすることもできます。
resetoutside	セキュリティ レベルが最も低いインターフェイスで終了し、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。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。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お勧めします。このキーワードを使用すると、外部の SMTP サーバまたは FTP サーバからの IDENT をセキュリティ アプライアンスで終端することができます。接続をアクティブにリセットすることにより、30 秒のタイムアウト遅延が回避されます。

デフォルト

デフォルトでは、**service resetoutbound** はすべてのインターフェイスでイネーブルになっています。

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。

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

識別要求（IDENT）接続をリセットする必要がある場合、着信トラフィックのリセットを明示的に送信することもできます。TCP RST（TCP ヘッダー内のリセット フラグ）を拒否されたホストに送信すると、RST により着信 IDENT プロセスが停止し、IDENT がタイムアウトになるまで待つ必要がなくなります。IDENT のタイムアウトを待っていると、トラフィックが遅くなることがあります。これは、IDENT がタイムアウトになるまで外部ホストが SYN の再送信を続けるためで、**service resetinbound** コマンドを使用するとパフォーマンスが向上することがあります。

例

次の例では、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しています。

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

次の例では、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しています。

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

次の例では、外部インターフェイス上で終了した接続のリセットをイネーブルにしています。

```
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 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、デフォルトではイネーブルになっています。ただし、不正なユーザがパスワードの回復メカニズムを利用してセキュリティ アプライアンスのセキュリティを侵害しないようにするために、この機能はディセーブルにすることをお勧めします。

service password-recovery

no service password-recovery

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

パスワードの回復は、デフォルトではイネーブルになっています。

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
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、起動中にプロンプトに従って端末キーボードの **Esc** キーを押すことで、セキュリティ アプライアンスで ROMMON に入ることができます。次に、コンフィギュレーション レジスタを変更して、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 である場合は、**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 アプライアンスをリロードするとデフォルト コンフィギュレーションがロードされるので、デフォルトのパスワードを使用して特権 EXEC モードに入ることができます。次に、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、以前と同様にブート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 アプライアンスの場合は、起動中にプロンプトに従って端末キーボードの **Esc** キーを押して、セキュリティ アプライアンスで監視モードに入ります。次に、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ます。このツールは、すべてのパスワードと **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、ユーザが設定目的で ROMMON に入ることを防止できます。ユーザが ROMMON に入ると、セキュリティ アプライアンスは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ユーザに要求します。ユーザは、最初にこの消去操作を実行しない限り、ROMMON に入ることができません。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。パスワードの回復では、ROMMON を使用すること、および既存のコンフィギュレーションを維持することが必要になるため、この消去操作を実行すると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、システムを動作可能な状態まで回復するには、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（入手できる場合）をロードします。**service password-recovery** コマンドがコンフィギュレーション ファイルに表示されるのは、情報の提供のみを目的としています。このコマンドを CLI プロンプトで入力すると、設定は NVRAM に保存されます。この設定を変更する唯一の方法は、このコマンドを CLI プロンプトで入力することです。このコマンドの別のバージョンを使用する新しい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。（パスワードの回復に備えて）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セキュリティ アプライアンスを設定している場合は、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 アプライアンスは設定を変更してスタートアップ コンフィギュレーションを通常どおりブートします。フェールオーバーを使用している場合、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を設定すると、**no service password recovery** コマンドがスタンバイ装置に複製されるときに、同じ変更がコンフィギュレーション レジスタに対して行われます。

PIX 500 シリーズ セキュリティ アプライアンス上で **no service password-recovery** コマンドを使用した場合は、PIX パスワード ツールを実行すると、ユーザは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要求されます。ユーザは、最初にこの消去操作を実行しない限り、PIX パスワード ツールを使用することができません。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。パスワードの回復では、既存のコンフィギュレーションを維持することが必要になるため、この消去操作を実行すると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、システムを動作可能な状態まで回復するには、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（入手できる場合）をロードします。

例

次の例では、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しています。

```
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.
```

次の例では、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しています。

```
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.
```

次の例は、ASA 5500 シリーズ適応型セキュリティ アプライアンス上で起動時に ROMMON に入るタイミングと、パスワードの回復操作を完了する方法を示しています。

```
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

すべてのインターフェイス上でグローバルに、または必要なインターフェイス上でポリシー 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。サーバ 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。インターフェイス上で一連のポリシー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*]

シンタックスの説明

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 マップのみ指定でき、検査ポリシー マップは指定できません（**policy-map type inspect**）。
global	ポリシー マップをすべてのインターフェイスに適用します。
interface *intf*	ポリシー マップを特定のインターフェイスに適用します。

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
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

インターフェイス サービス ポリシーはグローバル サービス ポリシーよりも優先されます。

デフォルトでは、コンフィギュレーションに、すべてのデフォルト アプリケーション検査トラフィックと一致し、検査をグローバルにトラフィックに適用するグローバル ポリシーが含まれます。適用できるグローバル ポリシーは 1 つのみです。このため、グローバル ポリシーの内容を変更する場合は、デフォルトのポリシーを編集するか、ディセーブルにして新しいものを適用する必要があります。

デフォルトのサービス ポリシーには、次のコマンドが含まれます。

```
service-policy global_policy global
```

例

次の例では、inbound_policy ポリシー マップを外部インターフェイスでイネーブルにする方法を示します。

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

次のコマンドは、デフォルトのグローバル ポリシーをディセーブルにし、new_global_policy という新しいポリシーを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
show service-policy	サービス ポリシーを表示します。
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。
clear service-policy	サービス ポリシーの統計情報を消去します。
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消去します。

session

AIP SSM または CSC SSM などのインテリジェント SSM 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***]

シンタックスの説明

do	*slot* 引数で指定された SSM 上でコマンドを実行します。Cisco TAC から指示がない限り、***do*** キーワードは使用しないでください。
ip	*slot* 引数で指定された SSM の IP アドレスのロギングを設定します。Cisco TAC から指示がない限り、***ip*** キーワードは使用しないでください。
slot	SSM スロット番号を指定します。これは、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
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*** キーワードと ***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 から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 がアップ状態のときにのみ使用できます。状態については、**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、**Ctrl+Shift+6** キーを押してから **X** キーを押します。

例

次の例では、スロット 1 で SSM へのセッションを確立しています。

```
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	セッションに関するデバッグ メッセージを表示します。

set connection

トラフィック クラスに関する接続値をポリシー マップ内で指定するには、クラス モードで **set connection** コマンドを使用します。このコマンドは、同時接続の最大数を指定するために、および TCP シーケンス番号のランダム化をイネーブルにするかどうかを指定するために使用します。これらの指定を削除して接続数を無制限にするには、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***}}. . . . .

シンタックスの説明

conn-max *n*	（オプション）許容される同時 TCP 接続または同時 UDP 接続の最大数。
disable	TCP シーケンス番号のランダム化をオフにします。
enable	TCP シーケンス番号のランダム化をオンにします。
embryonic-conn-max *n*	（オプション）許容される同時初期接続の最大数。
per-client-embryonic-max *n*	（オプション）許容される同時初期接続の最大数。
per-client-max *n*	（オプション）クライアントごとに許容される同時接続の最大数。
random-sequence-number	（オプション）TCP シーケンス番号のランダム化をイネーブルまたはディセーブルにします。

デフォルト

conn-max、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max*** の各パラメータの *n* のデフォルト値は 0 で、接続数は無制限になります。

シーケンス番号のランダム化は、デフォルトではイネーブルになっています。

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。
7.1(1)	***per-client-embryonic-max*** および ***per-client-max*** キーワードが追加されました。

使用上のガイドライン

conn-max、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max, random-sequence-number*** キーワードはいずれもオプションですが、少なくとも 1 つは指定する必要があります。

このコマンドに複数のパラメータを入力するか、個別のコマンドに各パラメータを入力することができます。セキュリティ アプライアンスは、実行コンフィギュレーションでこれらのコマンドを 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したとします。

```
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 つのコマンドが 1 つの結合されたコマンドという形で表示されます。

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

set connection コマンドのパラメータ（***conn-max***、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max***、***random-sequence-number***）は、任意の **nat** コマンドまたは **static** コマンドと共存できます。つまり、接続パラメータは **nat**/**static** コマンドで ***max-conn***、***emb_limit***、***noramdomseq*** の各パラメータを使用して設定することも、MPC の **set connection** コマンドで ***conn-max***、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max***、***random-sequence-number*** の各パラメータを使用して設定することもできます。混合コンフィギュレーションはお勧めしませんが、実際に使用した場合の動作は次のようになります。

- MPC の **set connection** コマンドと **nat**/**static** コマンドの両方でトラフィック クラスが接続制限または初期接続制限を課されている場合は、いずれか一方の制限値に達したときに、その制限値が適用されます。
- MPC の **set connection** コマンドまたは **nat**/**static** コマンドのいずれかで、シーケンス番号のランダム化をディセーブルにするように TCP トラフィック クラスが設定されている場合、シーケンス番号のランダム化はディセーブルになります。

per-client-embryonic-max パラメータおよび ***per-client-max*** パラメータは、クライアントが開くことのできる最大接続数を制限します。特定のクライアントが必要以上に多くのネットワーク リソースを同時に使用する場合、これらのパラメータを使用して、セキュリティ アプライアンスが特定のクライアントに許可する接続数を制限することができます。DoS 攻撃は、基幹ホストに対し接続や接続要求といった過剰な負荷をかけることにより、ネットワークを妨害しようとします。***per-client-embryonic-max*** パラメータおよび ***per-client-max*** パラメータを使用して、DoS 攻撃を防止することができます。攻撃を受ける可能性のあるホストがサポートできる、クライアントごとの最大接続数を設定すると、悪意のあるクライアントは保護されたネットワーク上のホストを攻撃できなくなります。

例

次の例では、**set connection** コマンドを使用して、同時接続の最大数を 256 に、TCP シーケンス番号のランダム化をディセーブルにするように設定しています。

```
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)#
```

次の例では、トラフィックを Cisco Content Security and Control（CSC）SSM に転送するサービス ポリシーで **set connection** コマンドを使用しています。**set connection** コマンドは、CSC SSM にトラフィックをスキャンされる各クライアントの接続を最大 5 つに制限します。

```
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)#
```

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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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 ポリシーのコンフィギュレーションを表示します。**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*

シンタックスの説明

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

次の例では、**set connection advanced-options** コマンドを使用して、localmap という TCP マップを使用することを指定しています。

```
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、多くとも 1 つの match コマンド（tunnel-group と default-inspection-traffic は除く）を発行し、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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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。

set connection timeout

アイドル状態の TCP 接続が切断されるまでのタイムアウト期間を設定するには、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 {**tcp** <*value*> [reset]] [**half-close** <*value*>] [**embryonic** <*value*>] [**dcd** [<retry-interval> [max-retries]]]}

no set connection timeout {**tcp** <*value*> [reset]] [**half-close** <*value*>] [**embryonic** <*value*>] [**dcd** [<retry-interval> [max-retries]]]}

シンタックスの説明

dcd	アイドル タイムアウトになると、DCD プローブを接続エンド ホストに送信して、接続の有効性を判断します。設定されている数の DCD プローブが設定されている間隔で送信された後、エンド ホストのいずれかが応答に失敗した場合、その接続は解放されます。両方のエンド ホストが接続が有効であると応答した場合、アクティビティ タイムアウトが現在の時刻に更新され、それに応じてアイドル タイムアウトのスケジュールも再設定されます。
embryonic	TCP 初期接続が終了するまでの絶対時間を設定します。1 ～ 255（秒）を設定します。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。
half-closed	TCP ハーフクローズ接続が解放されるまでのアイドル時間を設定します。5 ～ 255（分）を設定します。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。
max-retries	接続が「無効」と宣言されるまでに連続して失敗したリトライ数です。最小値は 1、最大値は 255 です。
reset	TCP アイドル接続が削除された後に、両端のシステムに TCP RST パケットを送信します。
retry-interval	非応答 DCD プローブ間の待機時間は <hh:mm:ss> 形式で表示します。最小値は 1 秒、最大値は 24 時間です。
tcp	確立済みの接続が終了するまでのアイドル時間です。
value	0:0:5 から 1192:59:59 までの時間（*hh*:*mm*:*ss* 形式）。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。

デフォルト

デフォルトの ***embryonic*** 値は 30 秒です。

デフォルトの ***half-closed*** 値は 10 分です。

デフォルトの **max-retries** 値は 5 です。

デフォルトの **retry-interval** 値は 15 秒です。

デフォルトの ***tcp*** 値は 1 時間です。

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

このコマンドを発行するには、**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。

「初期」接続とは、3 ウェイ ハンドシェイクの完了していない TCP 接続です。***embryonic*** 接続タイムアウト値には、***0:0:0*** を使用して接続がタイムアウトしないことを指定します。このように指定しない場合は、タイムアウト期間を 5 秒以上に設定する必要があります。

TCP 接続が終了中（CLOSING）状態のときは、half-closed パラメータを使用して、接続が解放されるまでの時間の長さを設定します。接続がタイムアウトしないように指定するには、***0:0:0*** を使用します。最短のタイムアウト期間は 5 分です。

tcp 非アクティブ接続のタイムアウトには、確立済み状態でアイドルになっている TCP 接続が切断されるまでの期間を設定します。接続がタイムアウトしないように指定するには、***0:0:0*** を使用します。最短のタイムアウト期間は 5 分です。

reset キーワードは、アイドル TCP 接続がタイムアウトしたときに両端のシステムに TCP RST パケットを送信する場合に使用します。アプリケーションの中には、タイムアウト後に TCP RST を送信しないと適切に動作しないものがあります。

DCD をイネーブルにすると、TCP ノーマライザにおけるアイドル タイムアウト処理の動作が変わります。Dead Connection Detection（DCD; デッド接続検出）プローブにより、**show conn** コマンドで表示される接続のアイドル タイムアウトがリセットされます。timeout コマンドで設定されているタイムアウト値を超えても、DCD プローブによって接続が維持される期間を判断するために、**show service-policy** コマンドには、DCD からアクティビティ量を表示するためのカウンタがあります。

例

次の **set connection timeout** コマンドの例では、初期接続のタイムアウトとして 2 分を指定しています。

```
ASA Version 7.2(0)80
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.0.0 standby 192.168.0.2
!
interface Vlan2
 backup interface Vlan4
 nameif outside
 security-level 0
 ip address 17.12.9.1 255.255.0.0 standby 17.12.9.2
!
interface Vlan4
 nameif backifx
 security-level 0
 ip address 172.23.62.137 255.255.255.0 standby 172.23.62.136
!
interface Vlan150
 description LAN Failover Interface
!
interface Vlan160
 nameif dmz
 security-level 50
 ip address 172.16.0.1 255.255.0.0 standby 172.16.0.2
!
interface Ethernet0/0
 switchport access vlan 2
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/2
 switchport access vlan 160
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/4
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/5
 switchport access vlan 150
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/6
 switchport access vlan 4
```

```
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/7
 switchport access vlan 4
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/cdisk.7.2.0.80
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list outside-acl extended permit ip any any
access-list inside_nat0_outbound extended permit ip any 192.168.0.128 255.255.25
5.192
access-list outside_cryptomap extended permit ip any 192.168.0.128 255.255.255.1
92
pager lines 24
logging enable
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu backifx 1500
mtu dmz 1500
ip local pool vpnpool 192.168.0.150-192.168.0.160 mask 255.255.0.0
no failover
failover lan unit primary
failover lan interface fover Vlan150
failover interface ip fover 150.1.1.1 255.255.255.0 standby 150.1.1.2
asdm image disk0:/asdm-5211.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 17.12.9.51 192.168.0.3 netmask 255.255.255.255
static (inside,outside) 17.12.9.52 192.168.0.10 netmask 255.255.255.255
static (inside,outside) 17.12.9.54 192.168.0.4 netmask 255.255.255.255
static (inside,dmz) 172.16.0.13 192.168.0.3 netmask 255.255.255.255
static (inside,dmz) 172.16.0.14 192.168.0.100 netmask 255.255.255.255
static (dmz,outside) 17.12.9.53 172.16.0.20 netmask 255.255.255.255
access-group outside-acl in interface outside
access-group outside-acl in interface dmz
route outside 0.0.0.0 0.0.0.0 17.12.0.1 1 track 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02      ------------>
ramain same
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy vpngroup internal
group-policy vpngroup attributes
 wins-server value 171.69.2.87
 dns-server value 171.70.168.183
 vpn-tunnel-protocol IPSec
 default-domain value cisco.com
username snoopy password wQO7//ZyQYDXv5q. encrypted privilege 15
aaa authentication telnet console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
http 192.168.0.0 255.255.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
sla monitor 10
 type echo protocol ipIcmpEcho 17.12.0.1 interface outside
 frequency 5
sla monitor schedule 10 life forever start-time now
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside0 20 set transform-set ESP-3DES-SHA
crypto map outside 20 ipsec-isakmp dynamic outside0
crypto map outside interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 10 reachability
tunnel-group vpngroup type ipsec-ra
tunnel-group vpngroup general-attributes
 address-pool vpnpool
 default-group-policy vpngroup
tunnel-group vpngroup ipsec-attributes
 pre-shared-key *
telnet 0.0.0.0 0.0.0.0 inside
telnet 0.0.0.0 0.0.0.0 outside
telnet timeout 5
ssh timeout 5
console timeout 0

!
class-map dcd
 match access-list outside-acl
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
 class dcd
  set connection timeout dcd
!
service-policy global_policy global
tftp-server outside 17.12.9.152 test1.cfg
prompt hostname context
Cryptochecksum:dc412a5fe2003621d7d723420da6e8d5
: end
ciscoasa(config)#
```

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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
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	DCD のカウンタおよびその他のサービス アクティビティを表示します。

set metric

ルーティング プロトコルに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 **set 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*

シンタックスの説明

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
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のものです。

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。この場合の *value* は、0 ～ 4294967295 の整数です。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
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、すべてのルートを再配布します。
match ip next-hop	指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、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ための条件を定義します。

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

シンタックスの説明

type-1	指定した自律システム外部の OSPF メトリック ルートのタイプを指定します。
type-2	指定した自律システム外部の 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
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のものです。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
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、すべてのルートを再配布します。
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ための条件を定義します。
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

対話型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によって、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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のものです。

使用上のガイドライン

フラッシュ メモリ内にスタートアップ コンフィギュレーションが存在しない場合、ブート時にセットアップ ダイアログが自動的に表示されます。

setup コマンドを使用するには、内部インターフェイスをあらかじめ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（Ethernet 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ついて、**interface** コマンドを入力し、次に **nameif inside** コマンドを入力しておく必要があります。

マルチ コンテキスト モードでは、システム実行スペース内で、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 に示す情報の入力を要求されます。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。要求されたパラメータに対するコンフィギュレーションがすでに存在している場合は、そのコンフィギュレーションが（）で囲まれて表示されます。このコンフィギュレーションをデフォルトとして受け入れることも、新しいコンフィギュレーションを入力して上書きすることもできます。

表 24-1　setup のプロンプト

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、セットアップ ダイアログが続行されます。***no*** を入力した場合、セットアップ ダイアログは停止して、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。このパスワードは、3 文字以上にする必要があります。
`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一切入力できません。デフォルトの UTC 時刻が使用されます。
`Year:`	西暦年を 4 桁で入力します（たとえば、2005）。年の範囲は 1993 ～ 2035 です。
`Month:`	月を表す英単語の先頭 3 文字を使用して、月を入力します。たとえば、**Sep** は 9 月を表します。
`Day:`	1 ～ 31 の日を入力します。
`Time:`	時、分、秒を 24 時間形式で入力します。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、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 アプライアンスが実行され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のあるホストの 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** と入力すると、内部インターフェイスがイネーブルとなり、要求し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*** と入力すると、セットアップ ダイアログが繰り返され、最初の質問が開始されます。 `Pre-configure Firewall now through interactive prompts [yes]?` ***no*** を入力してセットアップ ダイアログを終了するか、***yes*** を入力してセットアップ ダイアログを繰り返します。

例

次の例は、**setup** コマンド プロンプトで最後まで作業する方法を示しています。

```
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。

show aaa local user

現在ロックされているユーザ名のリスト、またはユーザ名に関する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 **show aaa local user** コマンドを使用します。

show aaa local user [locked]

シンタックスの説明

locked	（オプション）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
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 アプライアンスは、すべての AAA ローカル ユーザについて、失敗した試行とロックアウト ステータスの詳細を表示します。

username オプションを使用してユーザを 1 人のみ指定することも、***all*** オプションを使用してすべてのユーザを指定することもできます。

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を及ぼします。

管理者は、デバイスからロックアウトされません。

例

次の例では、**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 ステータスを表示しています。

この例では、認証失敗の上限を 5 回に設定した後で、**show aaa local user** コマンドを使用して、すべての AAA ローカル ユーザについて認証の失敗回数とロックアウト ステータスの詳細を表示しています。

```
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)#
```

次の例では、認証失敗の上限を 5 回に設定した後で、**show aaa local user** コマンドを ***lockout*** キーワード付きで使用して、ロックアウトされたすべての AAA ローカル ユーザについて、認証の失敗回数とロックアウト ステータスの詳細を表示しています。

```
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	正しくないパスワードの入力を何回まで許容するかを設定します。この回数を超えると、ユーザはロックアウトされます。
clear aaa local user fail-attempts	試行の失敗回数を 0 にリセットします。ロックアウト ステータスは変更しません。
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 ステータスを消去し、試行失敗のカウンタを 0 に設定します。

show aaa-server

AAA サーバに関する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*]

シンタックスの説明

LOCAL	（オプション）LOCAL ユーザ データベースの統計情報を表示します。
groupname	（オプション）グループに含まれているサーバの統計情報を表示します。
host *hostname*	（オプション）グループに含まれている特定のサーバの統計情報を表示します。
protocol *protocol*	（オプション）指定したプロトコルのサーバの統計情報を表示します。 • **http form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトでは、すべての AAA サーバの統計情報が表示されます。

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
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のものです。
7.1(1)	http 形式のプロトコルが追加されました。

例

次の例では、**show aaa-server** コマンドを使用して、サーバグループ group1 に含まれている特定のホストの統計情報を表示しています。

```
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/FAILED. Last transaction (success) at 11:10:08 UTC  Fri Aug
22
Number of pending requests 20
Average round trip time4ms
Number of authentication requests20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions1
Number of accepts  16
Number of rejects  4
Number of challenges   5
Number of malformed responses0
Number of bad authenticators0
Number of pending requests0
Number of timeouts 0
Number of unrecognized responses0
hostname(config)#
```

次の例では、**show aaa-server** コマンドを使用して、非アクティブな小規模システムに含まれているすべてのホストの統計情報を表示しています。

```
hostname(config)# show aaa-server
Server Group:      LOCAL
Server Protocol:   Local database
Server Address:    None
Server port:       None
Server status:     ACTIVE, Last transaction at unknown
Number of pending requests        0
Average round trip time           0ms
Number of authentication requests 0
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         0
Number of accepts                 0
Number of rejects                 0
Number of challenges              0
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
hostname(config)#
```

関連コマンド

show running-config aaa-server	指定したサーバグループに含まれているすべてのサーバ、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 サーバの統計情報を消去します。

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*

シンタックスの説明

id	アクセス リストを指定します。

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
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のものです。

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。

関連コマンド

コマンド	説明
access-list ethertype	トラフィックを EtherType に基づいて制御するためのアクセス 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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
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

アクティベーション キーによってイネーブルになった機能のコンフィギュレーションに含まれているコマンドを、許容されているコンテキストの数を含めて表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。

show activation-key

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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
PIX バージョン 7.0	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show activation-key コマンドの出力で示されるアクティベーション キーのステータスは、次のとおりです。

- セキュリティ アプライアンスのフラッシュ ファイル システムにあるアクティベーション キーが、セキュリティ アプライアンスで機能しているアクティベーション キーと同じものである場合、**show activation-key** コマンド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 システムにあるアクティベーション キーが、セキュリティ アプライアンスで機能しているアクティベーション キーと異なるものである場合、**show activation-key** コマンド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場合は、機能しているキー（古いキー）が、フラッシュに格納されているキー（新しいキー）と異なっていることが表示されます。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。
- キーをアップグレードして追加の機能をイネーブルにする場合、新しいキーはすぐに機能し始めます。再起動する必要はありません。
- PIX Firewall プラットフォームでは、新しいキーと古いキーでフェールオーバー機能（R/UR/FO）に違いがある場合、確認するように要求されます。ユーザが ***n*** を入力すると、変更内容は破棄されます。その他の場合は、フラッシュ ファイル システムに格納されているキーがアップデートされます。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。

例

次の例は、アクティベーション キーによってイネーブルになった機能のコンフィギュレーションに含まれているコマンドを表示する方法を示しています。

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada

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

The flash activation key is the SAME as the running key.
hostname(config)#
```

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 admin-context

管理コンテキストとして現在割り当てられているコンテキストの名前を表示するには、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
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。この例では、flash のルート ディレクトリに格納されている「admin」という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

アドレス解決プロトコル（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。このコマンドは、ダイナミック ARP エントリと手作業で設定した ARP エントリを表示しますが、各エントリの作成元は示しません。

show arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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のものです。

例

次に、**show arp** コマンドの出力例を示します。

```
hostname# show arp
        inside 10.86.195.205 0008.023b.9892
        inside 10.86.194.170 0001.023a.952d
        inside 10.86.194.172 0001.03cf.9e79
        inside 10.86.194.1 00b0.64ea.91a2
        inside 10.86.194.146 000b.fcf8.c4ad
        inside 10.86.194.168 000c.ce6f.9b7e
```

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	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去します。
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 検査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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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 カラムは、ARP 検査がイネーブルになっている場合に、一致しないパケットに対して実行するデフォルト アクション（flood または no-flood）を示しています。

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	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去します。
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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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のものです。

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 24-2 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の数。
Maximum queued blocks	IP アドレスが解決されるまで待機している間に、ARP モジュールのキューに入れられたブロックの最大数。
Queued blocks	ARP モジュールのキューに現在入っているブロックの数。
Interface collision ARPs received	すべてのセキュリティ アプライアンス インターフェイス上で、セキュリティ アプライアンス インターフェイスと同じ IP アドレスから受信した ARP パケットの数。

表 24-2　show arp statistics のフィールド（続き）

フィールド	説明
ARP-defense gratuitous ARPs sent	セキュリティ アプライアンスによって、ARP 防御メカニズムの一部として送信された gratuitous ARP の数。
Total ARP retries	最初の ARP 要求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た ARP 要求の合計数。
Unresolved hosts	ARP モジュールによってまだ ARP 要求が送信されている、未解決ホストの数。
Maximum unresolved hosts	未解決ホストが最後に消去された時点、またはセキュリティ アプライアンスがブートアップされた時点から、ARP モジュール内で未解決となったホスト数の最大値。

関連コマンド

コマンド	説明
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去し、値を 0 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***]

シンタックスの説明

asdmclient	（オプション）ASDM クライアント用に整形された ASDM 履歴データを表示します。
feature *feature*	（オプション）履歴の表示対象を指定された機能に限定します。次に、*feature* 引数で有効となる値を示します。 • ***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 使用率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名です。 • ***memory***：メモリ使用率の履歴を表示します。 • ***perfmon***：パフォーマンスの履歴を表示します。 • ***sas***：セキュリティ結合の履歴を表示します。 • ***tunnels***：トンネルの履歴を表示します。 • ***xlates***：変換スロットの履歴を表示します。
snapshot	（オプション）ASDM 履歴の最新データ ポイントだけを表示します。
view *timeframe*	（オプション）履歴の表示対象を指定された期間に限定します。次に、*timeframe* 引数で有効となる値を示します。 • ***all***：履歴バッファのすべての内容（デフォルト） • ***12h***：12 時間 • ***5d***：5 日間 • ***60m***：60 分間 • ***10m***：10 分間

デフォルト

引数もキーワードも指定しない場合は、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
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には、**asdm history enable** コマンドを使用して、ASDM 履歴のトラッキングをあらかじめイネーブルにしておく必要があります。

例

次に、**show asdm history** コマンドの出力例を示します。ここでは、出力する内容を外部インターフェイスに関する最近 10 分間に収集されたデータに限定しています。

```
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。上の例と同様に、出力する内容を外部インターフェイスに関する最近 10 分間に収集されたデータに限定しています。ただし、この例では出力を ASDM クライアント用に整形しています。

```
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|624
64|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|6
2628|62633|62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|627
04|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|250
25|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|2
5161|25165|25169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|253
67|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|751|751|751|751|751|751|751|751|7
51|751|751|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|752|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|39
79|4381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|484
7|4292|5401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|630
9|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|3
343|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|3
349|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|
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|
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|37
5373|375395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|3757
38|375761|375794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115
|376147|376168|376200|376224|376253|376289|376315|376365|376400|376436|376463|376508|3
76530|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|
```

```
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|
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|
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|
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|
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|
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|
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|
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|1
28|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|
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|
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|
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|
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 履歴の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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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 セッションのリスト、およびそれらのセッションに関連付けられているセッション ID 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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

アクティブな各 ASDM セッションは、1 つまたは複数の ASDM ロギング セッションと関連付けられています。ASDM は、このロギング 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 が割り当てられています。このセッション ID を **asdm disconnect log_session** コマンドで使用すると、指定したセッションを終了することができます。

（注）　各 ASDM セッションは、少なくとも 1 つの ASDM ロギング セッションを保持しているため、**show asdm sessions** と **show asdm log_sessions** の出力は同じ内容になることもあります。

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 セッションのリスト、およびそれらに関連付けられているセッション ID 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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 が割り当てられています。このセッション ID を **asdm disconnect** コマンドで使用すると、指定したセッションを終了することができます。

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。