CHAPTER 24

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

same-security-traffic

セキュリティ レベルが同じインターフェイス間での通信を許可したり、同一インターフェイスでトラフィックの着信および発信を許可するには、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。セキュリティが同じ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**}

シンタックスの説明

inter-interface	セキュリティ レベルが同じインターフェイス間の通信を許可します。
intra-interface	同一インターフェイスで着信と発信を行う通信を許可します。

デフォルト

デフォルトでは、この動作はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドに inter-interface キーワードが追加されました。
2.3(1)	intra-interface 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

セキュリティが同じ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）、101 を超える通信インターフェイスを設定できます。インターフェイスごとに異なるレベルを使用する場合、各レベル（0 ～ 100）で設定できるインターフェイスは 1 つだけです。

NAT 制御をイネーブルにする場合は、セキュリティ レベルの同じインターフェイス間で NAT を設定する必要はありません。

same-security-traffic intra-interface コマンドを使用すると、同一インターフェイスでトラフィックの発信と着信を行うことができます。これは、通常は許可されない動作です。

（注） 外部インターフェイス（たとえば、インターネットにアクセスする場合）のセキュリティ レベルを内部インターフェイスと同じレベルにすることは推奨しません。FWSM では、すべての接続に xlate エントリが関連付けられます（明示的に NAT を設定していない場合も含みます）。xlate は通常、内部インターフェイスと、セキュリティ レベルの低いインターフェイスとの接続用に作成されます。same-security-traffic 同一セキュリティ レベル トラフィック設定では、FWSM は、xlate を作成するために、どの同一セキュリティ レベル インターフェイスが「内部」インターフェイスなのかをランダムに選択します。リロード後、またはソフトウェア アップグレード後に、同じインターフェイスが選択されるとはかぎりません。FWSM が外部の同一セキュリティ レベル インターフェイスを「内部」インターフェイスとみなしてしまうと、そのインターフェイスを介してアクセスされるすべてのインターネット ホスト用に xlate が作成されます。

内部ネットワーク上に数千のインターネット ホストをスキャンするアプリケーション（あるいはウイルス）が存在していると、xlate テーブル内の全エントリを使い切ってしまいます（xlate の制限については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください）。そうなると、FWSM は新規の xlate を作成しなくなり、すべての新規接続に対して、エラー メッセージ %FWSM-3-305006:（translation creation failed [トランスレーションの作成に失敗しました]）がログに記録されます。**show resource usage** コマンドは、上限に達したかそれに近いアクティブな xlate の数を表示します。**clear xlate** コマンドは、接続を一時的に回復します。

こうした状況を回避するため、外部インターフェイスのセキュリティ レベルは常に、他のすべての FWSM インターフェイスよりも低く設定することを推奨します。このように設定することで、FWSM は常に、ISP リンクを外部インターフェイスとみなすようになります。その場合、ネットワーク内部からインターネット ホストをスキャンするアプリケーションまたはウイルスごとに、xlate が 1 つだけ作成されます。スキャンされるすべてのインターネット ホストに対して xlate が作成されることはありません。

例

次に、セキュリティが同じインターフェイス間で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、同一インターフェイスでトラフィックの発信と着信を許可する例を示します。

```
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** の設定を表示します。

sdi-pre-5-slave

SDI バージョン 5 より古い SDI を使用するこのホスト接続用に、オプションの SDI AAA「スレーブ」サーバの IP アドレスまたは名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sdi-pre-5-slave** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

sdi-pre-5-slave *host*

no sdi-pre-5-slave

シンタックスの説明

host	スレーブ サーバ ホストの名前または IP アドレスを指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは SDI AAA サーバ グループの任意のホストに使用できますが、意味を持つのは、**sdi-version** コマンドでホストの SDI バージョンが sdi-pre-5 に設定されている場合だけです。このコマンドを使用する前に、SDI プロトコルを使用するように AAA サーバを設定しておく必要があります。

sdi-pre-5-slave コマンドを使用すると、プライマリ サーバで障害が発生した場合に使用する、オプションのセカンダリ サーバを指定できます。このコマンドで指定するアドレスは、プライマリ SDI サーバに対する「スレーブ」として設定されたサーバのアドレスにする必要があります。この状況でバージョン 5 より前のバージョンを使用する場合は、**sdi-pre-5-slave** コマンドを設定し、FWSM がサーバからダウンロードされる適切な SDI コンフィギュレーション レコードにアクセスできるようにする必要があります。これは、バージョン 5 以降のバージョンには当てはまりません。

例

次に、SDI バージョン 5 より古い SDI を使用する、AAA SDI サーバ グループ [svrgrp1] の設定例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# sdi-version sdi-pre-5
hostname(config-aaa-server-host)# sdi-pre-5-slave 209.165.201.31
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA サーバ コンフィギュレーションを削除します。
sdi-version	このホスト接続に使用する SDI のバージョンを指定します。
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について、AAA サーバの統計情報を表示します。

sdi-version

このホスト接続に使用する SDI のバージョンを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sdi-version** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

sdi-version *version*

no sdi-version

シンタックスの説明

version	使用する SDI のバージョンを指定します。有効値は次のとおりです。 • ***sdi-5*** **—** SDI version 5.0（デフォルト） • ***sdi-pre-5*** **—** 5.0 より前の SDI バージョン

デフォルト

デフォルトのバージョンは ***sdi-5*** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドが有効なのは、SDI AAA サーバに限定されます。セカンダリ（フェールオーバー）SDI AAA サーバを設定し、なおかつそのサーバの SDI バージョンが 5 より古い場合、**sdi-pre-5-slave** コマンドも指定する必要があります。

例

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コンフィギュレーションを削除します。
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について、AAA サーバの統計情報を表示します。

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 ユニット認証の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。このオプションにより、別のグループ ポリシーからセキュア ユニット認証の値が継承されます。

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

no secure-unit-authentication

シンタックスの説明

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

セキュア ユニット認証は、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による認証をクライアントに要求することによって、セキュリティを強化します。この機能をイネーブルにした場合、ハードウェア クライアントは保存されたユーザ名とパスワードを使用しません。

（注） この機能がイネーブルのときに VPN トンネルを起動するには、ユーザ名とパスワードを入力するユーザが存在していなければなりません。

セキュア ユニット認証を使用するには、ハードウェア クライアント（複数可）が使用するトンネル 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 FWSM 上でセキュア ユニット認証が必要な場合は、必ず、バックアップ サーバでもセキュア 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	ユーザ認証を行わなくても IP Phone を接続できるようにします。Secure Unit Authentication は引き続き有効です。
leap-bypass	VPN ハードウェア クライアントの背後にある無線装置から送信された LEAP パケットが、ユーザ認証（イネーブルの場合）の前に VPN トンネルを通過するようにします。このようにすると、シスコ製無線アクセス 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。その後、ユーザ認証ごとに再認証します。
user-authentication	ハードウェア クライアントの背後にいるユーザに、FWSM の認証を受けてから接続することを要求します。

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値に戻すには、このコマンドの **no** 形式を使用します。セキュリティ レベルは、セキュリティの高いネットワークと低いネットワーク間の保護を強化することによって、セキュリティの低いネットワークから高いネットワークを保護します。

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

セキュリティ レベルはデフォルトで 0 です。

「内部」インターフェイスを指定し、セキュリティ レベルを明示的に設定しなかった場合、FWSM によってセキュリティ レベルが 100 に設定されます（**nameif** コマンドの項を参照）。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	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。**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 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を制御します。

- 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 レベルに従属します。セキュリティが同じインターフェイスの場合、インスペクション エンジンは双方向のトラフィックに適用されます。
  - NetBIOS インスペクション エンジン — 発信接続だけに適用されます。
  - OraServ インスペクション エンジン — ホスト ペアの間に OraServ ポートの制御接続が存在する場合、着信データ接続に限り、FWSM を通過することが許可されます。
- フィルタリング — HTTP（S）および FTP フィルタリングは、発信接続だけに適用されます（上位レベルから下位レベル）。

  セキュリティが同じインターフェイスの場合、双方向で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していて、セキュリティの高いインターフェイス（内部）上のホストからセキュリティの低いインターフェイス（外部）上のホストにアクセスする場合、セキュリティの高いインターフェイス上のホストに NAT を設定する必要があります。

  NAT 制御を使用しない場合、またはセキュリティが同じインターフェイスの場合は、任意のインターフェイス間で NAT を使用するかしないかを選択できます。外部インターフェイスに NAT を設置する場合、特殊なキーワードが必要になることがあります。
- **estabilied** コマンド — このコマンドを使用すると、セキュリティ レベルの高いホストから低いホストへの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高いホストへの復帰接続が可能です。

  セキュリティが同じインターフェイスの場合、双方向で **establised** コマンドを設定できます。

通常、セキュリティ レベルが同じインターフェイス間では通信できません。セキュリティ レベルが同じインターフェイス間の通信を可能にする場合は、**same-security-traffic** コマンドの項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場合、または同等に保護される部門が 2 つあるような状況で、2 つのインターフェイス間のトラフィックに保護機能を等しく適用する場合は、2 つのインターフェイスに同じレベルを割り当て、相互間で通信できるようにします。

インターフェイスのセキュリティ レベルを変更し、既存の接続がタイムアウトしないうちに新しいセキュリティ情報が使用されるようにする場合は、**clear local-host** コマンドを使用して接続を消去できます。

例　次に 2 つのインターフェイスについて、セキュリティ レベルを 100 および 0 に設定する例を示します。

```
hostname(config)# interface gigabitethernet0
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 gigabitethernet1
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。
nameif	インターフェイス名を設定します。

serial-number

登録時の証明書に FWSM のシリアル番号を含めるには、crypto 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、引数またはキーワードはありません。

デフォルト

シリアル番号を含めないのがデフォルトの設定です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
crypto 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
3.1(1)	このコマンドが追加されました。

例

次に、トラストポイント central の crypto 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、トラストポイント central に対する登録要求に FWSM 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
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 モードを開始します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、サーバ ポート番号 8888 を使用するように、[svrgrp1] という SDI AAA サーバを設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 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	すべての AAA サーバ コンフィギュレーションを削除します。
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について、AAA サーバの統計情報を表示します。

service resetinbound

拒否された着信 TCP 接続にリセットを送信するには、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。リセットを送信しないようにするには、このコマンドの **no** 形式を使用します。

service resetinbound

no service resetinbound

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、リセットは送信されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

service コマンドは、アクセス リストまたは uauth（ユーザ許可）で着信接続が禁止されている、すべての着信 TCP 接続に対して機能します。用途としては、識別要求（IDENT）接続のリセットなどがあります。着信 TCP 接続が試行されて拒否された場合、**service resetinbound** コマンドを使用して、RST（TCP ヘッダー内のリセット フラグ）を送信元に返すことができます。キーワードを指定しなかった場合、FWSM は RST を返さずにパケットを廃棄します。

FWSM は着信接続ホストに TCP RST を送信し、着信 IDENT プロセスを停止することにより、発信電子メールが IDENT のタイムアウトを待たずに送信されるようにします。FWSM は、着信接続が拒否されたことを示す Syslog メッセージを送信します。**service resetinbound** コマンドを入力しなかった場合、FWSM は拒否されたパケットを廃棄し、SYN が拒否されたことを示す Syslog メッセージを生成します。ただし、外部ホストは IDENT がタイムアウトするまで SYN の再送信を続けます。

IDENT 接続がタイムアウトになると、接続速度が落ちます。トレースを実行して、速度低下の原因が IDENT であるかどうかを判断してから、**service** コマンドを入力します。

FWSM を介して IDENT 接続を処理するには、**service resetinbound** コマンドを使用します。次に、IDENT 接続の処理方法をセキュリティが高いものから順に示します。

1. **service resetinbound** コマンドを使用します。
2. **permitto tcp 113** キーワードを指定して、**established** コマンドを使用します。
3. **static** コマンドおよび **access-list** コマンドを入力して、TCP ポート 113 を開きます。

aaa コマンドを使用する場合、最初の許可試行が失敗し、次の試行でタイムアウトした場合は、**service resetinbound** コマンドを使用して許可に失敗したクライアントをリセットし、接続を再送信しないようにします。次に、Telnet での許可タイムアウト メッセージの例を示します。

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

リセット フラグに関して、FWSM 上で予期されるトラフィック動作は、次のとおりです。

1. ***resetinbound*** が設定されていて、なおかつセキュリティの低いインターフェイスから高いインターフェイスへのトラフィック フローが拒否される場合、リセットが送信されます。
2. ***resetinbound*** が設定されていて、なおかつセキュリティ レベルが同じインターフェイス間のトラフィック フローが拒否される場合、リセットが送信されます。
3. ***resetinbound*** が設定されていて、なおかつセキュリティの高いインターフェイスから低いインターフェイスへのトラフィック フローが拒否される場合、リセットが送信されます。

例

次に、システム サービスをイネーブルにする例を示します。

```
hostname(config)# service resetinbound
```

関連コマンド

コマンド	説明
show running-config service	システム サービスを表示します。

service-policy

すべてのインターフェイスでグローバルに、またはターゲット 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、特権 EXEC モードで ***service-policy*** コマンドを使用します。この設定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-policy*** コマンドは、インターフェイス上で 1 組のポリシーをイネーブルにする場合に使用します。***service-policy*** コマンドは通常、***nameif*** コマンドで定義可能なすべてのインターフェイスに適用できます。

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	英数字で表された一意のポリシー マップ ID
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	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。
intf	***nameif*** コマンドで定義されたインターフェイス名

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス名を指定した場合、ポリシー マップはそのインターフェイスだけに適用されます。インターフェイス名は ***nameif*** コマンドで定義します。インターフェイスのポリシー マップによって、グローバル ポリシー マップが上書きされます。1 つのインターフェイスに使用できるポリシー マップは 1 つだけです。

使用できるグローバル ポリシーは 1 つだけです。

例

次に、***service-policy*** コマンドの構文例を示します。

```
hostname(config)# service-policy outside_security_map outside
```

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で設定されたサービス 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 ポリシー設定を消去します。

set connection

トラフィック クラスにおける TCP および UDP 接続の最大数を設定したり、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たりするには、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。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスします。これらの指定を削除し、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** *number*] **[random-seq# {enable | disable}]}**

no set connection {[**conn-max** *number*] **[random-seq# {enable | disable}]}**

シンタックスの説明

***conn-max** number*	TCP および UDP 同時接続の最大数を設定します。
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。
random-seq#	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。別のインライン ファイアウォールで TCP シーケンス番号のランダム化をイネーブルにしている場合は、ランダム化をディセーブルにできます。両方のファイアウォールで同じ動作を実行する必要はないからです。ただし、ISN ランダム化については、両方のファイアウォールでイネーブルのままにしても、トラフィックに影響はありません。 各 TCP 接続には ISN が 2 つあります。1 つはクライアントによって生成され、もう 1 つはサーバによって生成されます。セキュリティ アプライアンスは、発信方向に渡される TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続では、SYN の ISN が両方向でランダム化されます。 保護されたホストで ISN をランダム化することにより、新規接続の次の ISN を予測して新規セッションをハイジャックする攻撃を阻止できます。

デフォルト

conn-max キーワードでは、*number* のデフォルト値は 0 です。この場合、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、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

class-map コマンドでトラフィックを特定してから、**policy-map** コマンドを入力して各クラス マップに対応するアクションを指定します。**class** コマンドを入力してクラス マップを指定し、さらに **set connection** コマンドを入力して、そのクラス マップの接続数を設定します。

（注）

NAT の設定（**nat** コマンドおよび **static** コマンド）で最大接続数および TCP シーケンス番号のランダム化を設定することもできます。両方の方法で同じトラフィックにこれらの値を設定した場合、FWSM は低い方の限度を使用します。TCP シーケンス番号のランダム化がどちらかの方法でディセーブルになっている場合、FWSM は TCP シーケンス番号のランダム化をディセーブルにします。

NAT では **set connection** コマンドと異なり、DoS 攻撃を防ぐために TCP 代行受信が起動される、初期接続限度も設定します。

例

次に、同時接続の最大数を 256 に設定し、TCP シーケンス番号の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-seq# disable
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップを指定します。
class-map	サービス ポリシーで使用するクラス マップを作成します。
policy-map	クラス マップと 1 つ以上のアクションを対応付ける、ポリシー マップを設定します。
service-policy	インターフェイスにポリシー マップを割り当てます。
set connection timeout	接続タイムアウトを設定します。

set connection timeout

初期、ハーフクローズド、またはアイドル状態の TCP 接続を切断するまでのタイムアウト期間を設定するには、クラス 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*] [**half-closed** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]]}

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

シンタックスの説明

embryonic *hh*:*mm*:*ss*	初期接続を終了するまでのタイムアウト期間を 0:0:1 ～ 0:4:15 の間で定義します。デフォルトは 0:0:20 秒です。0 を設定すると、接続タイムアウトが発生しなくなります。**set connection** コマンドで初期接続の最大数を設定することはできませんが、タイムアウトはこのコマンドで設定できます。
half-closed *hh*:*mm*:*ss*	TCP ハーフ クローズド接続を解放するまでのタイムアウト期間を 0:0:1 ～ 0:4:15 の間で定義します。デフォルトは 0:0:20 秒です。0 を設定すると、タイムアウトが発生しなくなります。
reset	（任意）接続タイムアウトが発生したら、TCP エンドポイントにリセットを送信します。FWSM は、ホストが（同じ送信元および宛先ポートで）タイムアウトを通知する別のパケットを送信場合のみ、それに応答してリセット パケットを送信します。そのホストは、リセット パケットを受信すると、接続テーブルから接続を削除します。これによりホスト アプリケーションは、SYN パケットを使用して新規接続を確立する操作を試行できます。
tcp *hh*:*mm*:*ss*	確立済み TCP 接続は所定のアイドル時間が経過すると終了します。このアイドル時間を 0:5:0 ～ 0:15:1092 の間で定義します。デフォルトは 0:60:0 です。0 を設定すると、接続タイムアウトが発生しなくなります。

デフォルト

デフォルトの **embryonic** 接続タイムアウト値は 20 秒です。

デフォルトの ***half-closed*** 接続タイムアウト値は 20 秒です。

デフォルトの ***tcp*** 接続タイムアウト値は 60 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

class-map コマンドでトラフィックを特定してから、**policy-map** コマンドを入力して各クラス マップに対応するアクションを指定します。**class** コマンドを入力してクラス マップを指定し、さらに **set connection timeout** コマンドを入力して、そのクラス マップの接続タイムアウトを設定します。

例

次に、TCP 接続のタイムアウトを 2 時間に設定する **set connection timeout** コマンドの例を示します。

```
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)# 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 timeout tcp 2:0:0
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップを指定します。
class-map	サービス ポリシーで使用するクラス マップを作成します。
policy-map	クラス マップと 1 つ以上のアクションを対応付ける、ポリシー マップを設定します。
service-policy	インターフェイスにポリシー マップを割り当てます。
set connection	TCP および UDP 接続の最大数を設定します。

set metric

宛先ルーティング 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 **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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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 ルーティングに関するルート マップの設定例を示します。

```
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	指定されたインターフェイスの 1 つを起点とするネクスト ホップのあるすべてのルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。

set metric

宛先ルーティング 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 **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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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 ルーティングに関するルート マップの設定例を示します。

```
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	指定されたインターフェイスの 1 つを起点とするネクスト ホップのあるすべてのルートを配布します。
match ip next-hop	指定のアクセス リストのいずれかと一致する、ネクストホップ ルータ アドレスが含まれるすべてのルートを配布します。
route-map	ルーティング プロトコル間でルートを再配布する条件を定義します。

setup

対話型プロンプトから FWSM 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** コマンドを使用します。

setup

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM に ASDM を接続するには、初期設定が必要です。**setup** コマンドを入力する前に、**nameif** コマンドを使用して、「内部」インターフェイスを指定する必要があります。FWSM には、デフォルトの内部インターフェイスはありません。

setup コマンドを入力すると、表 24-1 に示した設定情報を入力するように求められます。

表 24-1　設定情報

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*** を入力した場合は、セットアップ ダイアログが中止され、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。ファイアウォール モード プロンプトを使用できるのは、シングル モードまたはコンテキストに限られます。
`Enable password:`	イネーブル パスワードを入力します（パスワードには 3 文字以上を指定する）。
`Inside IP address:`	FWSM のネットワーク 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、255.255.0.0、または 255.255.x.x 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。デフォルト ルートを指定する場合は、0.0.0.0 を使用します。ネットマスク 0.0.0.0 の省略形として 0 を使用できます。

表 24-1　設定情報（続き）

`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:`	FWSM が動作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 が FWSM に接続する IP アドレスを入力します。
`Use this configuration and write to flash [yes]?`	***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、必要な設定がフラッシュ パーティションに書き込まれます。 ***no*** を入力した場合は、セットアップ ダイアログが最初の質問から繰り返されます。 `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、または ***yes*** を入力してセットアップ ダイアログを繰り返します。

ホスト名およびドメイン名は、Secure Socket Layer（SSL）接続用のデフォルト証明書を生成する場合に使用されます。

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
Inside IP address [192.168.1.1]: 192.168.1.1
Inside network mask [255.255.255.0]: 255.255.255.0
Host name [tech_pubs]: tech_pubs
Domain name [your_company.com]: your_company.com
IP address of host running Device Manager:

The following configuration will be used:
Enable password: writer
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

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

関連コマンド

コマンド	説明
asdm	FWSM とデバイス マネージャが動作しているブラウザ間の通信を設定します。

show aaa-server

AAA サーバの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*]

シンタックスの説明

LOCAL	（任意）LOCAL 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	このコマンドが LOCAL メソッドをサポートするように変更されました。

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 内の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. 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の説明を示します。

フィールド	説明
Server Group	**aaa-server** コマンドで指定したサーバ グループ名
Server Protocol	**aaa-server** コマンドで指定したサーバ 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	FWSM および AAA サーバが使用する通信ポート。RADIUS 認証ポートを指定するには、**authentication-port** コマンドを使用します。RADIUS アカウンティング ポートを指定するには、**accounting-port** コマンドを使用します。非 RADIUS サーバの場合は、**server-port** コマンドでポートを設定します。
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 — FWSM は、この AAA サーバと通信できます。 • FAILED — FWSM 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、そのままの状態で維持され、ポリシーによって規定された期間が経過すると再アクティブ化されます。 次の形式を使用すると、最後の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* FWSM がサーバと通信したことがない場合は、次のようなメッセージが表示されます。 **Last transaction at Unknown**
Number of pending requests	処理中の要求の数
Average round trip time	サーバとのトランザクションが終了するまでの平均所要時間。
Number of authentication requests	FWSM が送信した認証要求の数。タイムアウト後の再送信はカウントしません。

フィールド	説明
Number of authorization requests	権限付与要求の数。この値は、コマンド権限付与、（TACACS+ サーバの）through-the-box トラフィック権限付与、トンネル グループ用にイネーブルにされた IPSec 権限付与機能などの権限付与要求の数を意味します。タイムアウト後の再送信はカウントしません。
Number of accounting requests	アカウンティング要求の数。タイムアウト後の再送信はカウントしません。
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。このコマンドは、Kerberos サーバおよび TACACS+ サーバ（UDP）にのみ適用されます。
Number of accepts	許可された認証要求の数
Number of rejects	拒否された要求の数。AAA サーバから資格情報によって拒否された数だけでなく、エラー条件もカウントされます。
Number of challenges	最初にユーザ名とパスワード情報を受信したあと、AAA サーバがユーザから追加情報を要求した回数
Number of malformed responses	現在は未使用。予約フィールド
Number of bad authenticators	次のどちらかが発生した回数 • RADIUS パケット内のオーセンティケータ文字列が破損している（非常にまれ）。 • FWSM の共有秘密キーが、RADIUS サーバ上のキーと一致しない。この問題を修正するには、正しいサーバ キーを入力します。 RADIUS だけで使用します。
Number of timeouts	AAA サーバが応答していないか、不正な動作をしたため、FWSM によってオフラインであると宣言された回数
Number of unrecognized responses	FWSM が、AAA サーバから、認識またはサポートできないという応答を受信した回数。たとえば、サーバから返された RADIUS パケット コードが未知のタイプ、すなわち、既知のタイプ「access-accept」、「access-reject」、「access-challenge」、または「accounting-response」のいずれでもない場合。これは通常、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ますが、非常にまれなケースです。

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、または特定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 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、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**]

シンタックスの説明

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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

オプション キーワード ***locked*** を指定しなかった場合、FWSM 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 ステータスを表示します。

username オプションで特定のユーザを指定することも、または ***all*** オプションですべてのユーザを指定することもできます。

このコマンドが作用するのは、ロックアウトされているユーザのステータスだけです。

装置から管理者を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、すべてのユーザ名についてロックアウト ステータスを表示する例を示します。

この例では、**show aaa local user** コマンドを使用して、限度を 5 に設定したあとで、すべての AAA ローカル ユーザについて、認証に失敗した回数とロックアウト ステータスの詳細を表示します。

```
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       augry13
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

次に、***lockout*** キーワードを指定して **show aaa local user** コマンドを使用し、限度を 5 に設定したあとで、ロックアウトされている AAA ローカル ユーザに限定して、認証に失敗した回数とロックアウト ステータスの詳細を表示します。

```
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	ユーザがロックアウトされるまでに、無効なパスワードを入力できる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、失敗した試行回数を 0 にリセットします。
clear aaa local user lockout	特定ユーザまたは全ユーザのロックアウト ステータスを消去し、対応する失敗試行回数のカウンタを 0 に設定します。

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 リストを特定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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
```

出力には各行の末尾に ACE ごとに一意の 16 進数 ID が含まれています。

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	設定にアクセス リストを追加し、ファイアウォールを通過する IP トラフィック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 リストを消去します。
show running-config access-list	現在実行中のアクセス リスト設定を表示します。

show activation-key

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、許可されているコンテキスト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、引数またはキーワードはありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

show activation-key コマンドの出力は、次のように、アクティベーション キーのステータスを示します。

- FWSM 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 FWSM で稼働するアクティベーション キーが同じ場合、**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.
```

- FWSM 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 FWSM 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。FWSM 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。FWSM を再起動すると、新しいキーが使用されます。

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

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

現在、admin 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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

例

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

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

関連コマンド

コマンド	説明
admin-context	admin コンテキストを設定します。
changeto	コンテキストとシステム実行スペースを切り替えます。
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（システム実行スペース）リスト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。このコマンドを使用すると、ダイナミックおよび手動設定された ARP エントリが表示されます。ただし、各エントリの作成元は特定されません。

show arp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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	トランスペアレント ファイアウォール モードの場合に、ARP スプーフィングを防止するために ARP パケットを検査します。
clear arp statistics	ARP の統計情報を消去します。
show arp statistics	ARP の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設定を表示します。

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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

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 カラムには、ARP 検査がイネーブルの場合に、不一致パケットに対して実行するデフォルトのアクションが示されます。[flood] または [no-flood] のどちらかです。

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 モードの場合に、ARP スプーフィングを防止するために ARP パケットを検査します。
clear arp statistics	ARP の統計情報を消去します。
show arp statistics	ARP の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設定を表示します。

show arp statistics

ARP の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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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:
        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 で各フィールドについて説明します。

表 24-2　show arp statistics のフィールド

フィールド	説明
Number of ARP entries	ARP テーブルのエントリ総数
Dropped blocks in ARP	IP アドレスを対応するハードウェア アドレスに解決しているときに廃棄されたブロック数
Maximum queued blocks	IP アドレス解決待ちの間に、ARP モジュールでキューに格納さ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格納されているブロック数
Interface collision ARPs received	すべての FWSM インターフェイスで、FWSM 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
ARP-defense gratuitous ARPs sent	ARP 防御メカニズムの一部として FWSM が送信した gratuitous ARP の数

表 24-2　show arp statistics のフィールド（続き）

フィールド	説明
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ときに、ARP モジュールが送信した ARP 要求の総数
Unresolved hosts	ARP モジュールから ARP 要求が送信され続けている、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てから、または FWSM の起動後に、ARP モジュール内で未解決となったホストの最大数

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 モードの場合に、ARP スプーフィングを防止するために ARP パケットを検査します。
clear arp statistics	ARP の統計情報を消去して、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設定を表示します。

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	（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）指定した機能に履歴表示を限定します。*feature* 引数で有効な値は、次のとおりです。 • ***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* **—** 指定されたインターフェイスの履歴を表示します。*if_name* 引数は **nameif** コマンドで指定されたインターフェイスの名前です。 • ***memory*** **—** メモリ使用量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 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*** **—** 変換スロットの履歴を表示します。
snapshot	（任意）最新の ASDM 履歴データ ポイントだけを表示します。
view *timeframe*	（任意）指定した期間に履歴表示を限定します。*timeframe* 引数で有効な値は、次のとおりです。 • ***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 • ***10m*** **—** 10 分

デフォルト

引数またはキーワードを指定しなかった場合は、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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
1.1(1)	このコマンドが（**show pdm history** として）追加されました。
3.1(1)	**show pdm history** から **show asdm history** にコマンドが変更されました。

使用上のガイドライン

show asdm history コマンドを使用すると、ASDM 履歴バッファの内容が表示されます。ASDM の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。この出力は、直近 10 分間に収集された外部インターフェイスのデータに限定されています。

```
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。この出力も前の例と同様、直近 10 分間に収集された外部インターフェイスのデータに限定されています。ただし、ASDM クライアント用にフォーマットされた出力例です。

```
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|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|
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|
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|
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|
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|
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|
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|
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|
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|
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|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|
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|
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|
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|
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|
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 sessions

アクティブな ASDM セッションおよび対応するセッション 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

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが（**show pdm sessions** として）追加されました。
3.1(1)	**show pdm sessions** から **show asdm sessions** にコマンドが変更されました。

使用上のガイドライン

アクティブな ASDM セッションごとに一意のセッション ID が 1 つずつ割り当てられます。**asdm disconnect** コマンドでこのセッション ID を使用すると、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。