S のコマンド

same-security-traffic

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インターフェイス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	トラフィックが IPSec で保護されている場合に、同じインターフェイスでの通信（送受信）を許可します。

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。

コマンドのモード

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

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すると、次のような利点があります。

- 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。

着信するクライアント VPN トラフィックを、暗号化されているものと同様に、同じインターフェイスから暗号化しないまま外部にリダイレクトすることもできます。VPN トラフィックを同じインターフェイスを通じて暗号化しないまま外部に再発信する場合は、インターフェイスで NAT をイネーブルにして、パブリック ネットワークでルーティング可能なアドレスでプライベート IP アドレスを置き換える必要があります（ローカル IP アドレス プール内ですでにパブリック IP アドレスを使用している場合は除く）。次のコマンド例では、クライアント IP プールが送信元になっているトラフィックに対して、インターフェイス PAT 規則を適用しています。

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# global (outside) 1 interface
hostname config)# nat (outside) 1 192.168.0.0 255.255.255.0
```

ただし、暗号化された VPN トラフィックをこの同じインターフェイスを通じてセキュリティ アプライアンスが外部に再発信する場合、NAT はオプションです。すべての発信トラフィックに NAT を適用するには、上のコマンドのみを実装します。VPN 間トラフィックを NAT の対象外にするには、上の例に次のようなコマンドを追加して、VPN 間トラフィックに NAT 例外を実装します。

```
hostname(config)# access-list nonat permit ip 192.168.0.0 255.255.255.0 192.168.0.0
255.255.255.0
hostname(config)# nat (outside) 0 access-list nonat
```

詳細については、**nat** コマンドを参照してください。

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
```

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。

sdi-pre-5-slave

バージョン 5 より前の SDI を使用しているホスト接続で使用される、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

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SDI AAA サーバグループのすべてのホストに対して使用できます。ただし、このコマンドが作用するのは、ホストの SDI バージョンが **sdi-version** コマンドで sdi-pre-5 に設定されている場合のみです。このコマンドを使用するには、SDI プロトコルを使用するように AAA サーバをあらかじめ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される、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 サーバの「スレーブ」として設定されているサーバのアドレスにする必要があります。このため、バージョン 5 より前のバージョンを使用している場合は、**sdi-pre-5-slave** コマンドを設定して、（SDI 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 レコードにセキュリティ アプライアンスがアクセスできるようにする必要があります。バージョン 5 およびそれ以降のバージョンでは、この要件はありません。

例

次の例では、バージョン 5 より前の SDI バージョンを使用している AAA SDI サーバグループ「svrgrp1」を設定しています。

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

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA パラメータを設定できるようにします。
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。
sdi-version	このホスト接続で使用する 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の AAA サーバ統計情報を表示します。

sdi-version

ホスト接続で使用する 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。有効となる値は、次のとおりです。 ***sdi-5***：SDI バージョン 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 バージョンは、***sdi-5*** です。

コマンドのモード

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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SDI AAA サーバに対してのみ有効です。セカンダリ（フェールオーバー）SDI AAA サーバを設定する場合、そのサーバの SDI バージョンがバージョン 5 より前のときは、**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
hostname(config-aaa-server)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA パラメータを設定できるようにします。
clear configure aaa-server	AAA 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。

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。

コマンドのモード

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。

コマンドのモード

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。

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。

コマンドのモード

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。

コマンドのモード

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。

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。

コマンドのモード

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。

コマンドのモード

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

コマンドのモード

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)# exit
hostname(config)#
```

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。

コマンドのモード

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。

service

システム サービス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。システム サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

service {**resetinbound | resetoutside**}

no service {**resetinbound | resetoutside**}

シンタックスの説明

resetinbound	拒否された着信 TCP パケットに対するリセットを送信します。
resetoutside	拒否された、外部インターフェイスへの TCP パケットに対するリセットを送信します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

service コマンドは、アクセスリストまたは uauth（ユーザ認可）が着信接続を許可しないスタティック インターフェイスへの着信 TCP 接続すべてに対して機能します。用途の 1 つは、識別要求（IDENT）接続のリセットです。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い場合、セキュリティ アプライアンスは RST を返さずにパケットをドロップします。

セキュリティ アプライアンスは、着信接続ホストに TCP RST を送信し、着信 IDENT プロセスを停止して、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。セキュリティ アプライアンスは、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** を入力しない場合、セキュリティ アプライアンスは、拒否されたパケットをドロップし、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 がタイムアウトになるまで、SYN を再送信し続けます。

IDENT 接続がタイムアウトすると、接続で遅延が発生します。トレースを実行して、遅延の原因が IDENT であるかどうか判断してから、**service** コマンドを入力します。

セキュリティ アプライアンスで IDENT 接続を処理するには、**service resetinbound** コマンドを使用します。IDENT 接続を処理する方法には、次のものがあります。セキュリティの高い順にランク付けしています。

1. **service resetinbound** コマンドを使用する。
2. **established** コマンドを **permitto tcp 113** キーワードとともに使用する。
3. **static** コマンドと **access-list** コマンドを入力して、TCP ポート 113 を開く。

aaa コマンドを使用する場合、最初の認可試行が失敗し、次の試行でタイムアウトになったときには、**service resetinbound** コマンドを使用して、認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。次の例は、Telnet での認可タイムアウト メッセージを示しています。

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

次に、リセット フラグに対するセキュリティ アプライアンス上のトラフィックの想定動作を示します。

1. ***resetinbound*** が設定されている場合、拒否されたトラフィックが、セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに向かっているときは、リセットが送信される。
2. ***resetinbound*** が設定されている場合、拒否されたトラフィックが、あるインターフェイスからセキュリティ レベルの等しい別のインターフェイスに向かっているときは、リセットが送信される。
3. ***resetinbound*** が設定されていない場合、拒否されたトラフィックが、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に向かっているときは、リセットが送信される。

resetoutside コマンドを使用すると、セキュリティ アプライアンスは、セキュリティ アプライアンスのセキュリティ レベルの最も低いインターフェイスで終端する、拒否された TCP パケットをアクティブにリセットします。デフォルトでは、パケットは、通知なしで廃棄されます。**resetoutside** キーワードは、ダイナミックまたはスタティックのインターフェイス Port Address Translation（PAT; ポート アドレス変換）で使用することをお勧めします。スタティック インターフェイス PAT は、セキュリティ アプライアンス バージョン 6.0 以降で使用できます。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。

例

次の例は、システム サービスをイネーブルにする方法を示しています。

```
hostname/context_name(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 internal

通常は非表示になる、条件付きのコマンドをデバイスが表示できるようにするには、**service internal** コマンドを使用します。

service internal

[no] service internal

シンタックスの説明

service	FIPS システム サービスをイネーブルまたはディセーブルにします。
internal	高度な設定（シスコの指導の下でのみ使用）

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。

コマンドのモード

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(4)	このコマンドが導入されました。

使用上のガイドライン

service internal オプションを使用すると、通常の運用では必要のない追加コマンドにアクセスできます。「internal」とマークされたコマンドを service internal の実行前に実行しようとすると、そのコマンドは、存在しないコマンドを実行しようとした場合と同様に失敗します。警告バナーが表示され、「service internal 実行後にアンロックされるコマンドは、シスコの指導の下でのみ実行する必要がある」と通知されます。

例

```
hostname(config)# service internal
hostname(config)# show running-config service service internal
hostname(config)# no service internal
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS 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。

コマンドのモード

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 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、特権 EXEC モードで ***service-policy*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。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。通常、***service-policy*** コマンドは、***nameif*** コマンドで定義できるどのインターフェイスにも適用できます。

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	英数字で記述された一意のポリシーマップ識別子。
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	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。
intf	***nameif*** コマンドで定義したインターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名が指定されている場合、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 ポリシーマップは上書きされます。1 つのインターフェイスにつき 1 つのポリシーマップだけを適用できます。

グローバル ポリシーは 1 つしか適用できません。

例

次の例は、***service-policy*** コマンドのシンタックスを示しています。

```
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 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 *1*

シンタックスの説明

1	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。

コマンドのモード

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

このコマンドは、AIP 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またはディセーブルに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** | **embryonic-conn-max**} *n* **random-seq# {enable | disable}**

no set connection {**conn-max** | **embryonic-conn-max**} *n* **random-seq# {enable | disable}**

シンタックスの説明

conn-max n	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	許容される同時初期接続の最大数。
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。

デフォルト

conn-max パラメータと ***embryonic-conn-max*** パラメータの *n* のデフォルト値は両方とも 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。

コマンドのモード

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、**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。

（注）　**set connection** コマンドのパラメータ（***conn-max***、***embryonic-conn-max***、***random-seq#***）は、任意の **nat** コマンドおよび **static** コマンドと共存できます。つまり、接続パラメータは **nat** コマンドや **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***、***random-seq#*** 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。

例　次の例では、クラス モードで 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-seq# disable
hostname(config-pmap-c)# exit
```

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。
help policy-map	policy-map コマンド シンタックスのヘルプを表示します。
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 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。

コマンドのモード

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
```

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 tcp *hh*[:*mm*[:*ss*]] [**reset**]

no set connection timeout tcp

set connection timeout embryonic *hh*[:*mm*[:*ss*]]

no set connection timeout embryonic

set connection timeout half-closed *hh*[:*mm*[:*ss*]]

no set connection timeout half-closed

シンタックスの説明

embryonic *hh*[:*mm*[:*ss*]]	TCP 初期（ハーフオープン）接続を終了するまでのタイムアウト期間。
half-closed *hh*[:*mm*[:*ss*]]	TCP ハーフクローズ接続に許容されるタイムアウト期間で、経過後に TCP ハーフクローズ接続が解放されます。
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。
tcp *hh*[:*mm*[:*ss*]]	確立済みの接続に許容されるアイドル時間で、経過後に確立済みの接続が終了します。

デフォルト

デフォルトの ***embryonic*** 接続タイムアウト値は 30 秒です。

デフォルトの ***half-closed*** 接続タイムアウト値は 10 秒です。

デフォルトの ***tcp*** 接続タイムアウト値は 1 時間です。

コマンドのモード

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、**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 接続を切断す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。

例

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

```
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)# 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 embryonic 00:2:00
```

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。

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。

コマンドのモード

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。

コマンドのモード

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。

コマンドのモード

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 7-1 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 7-1　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。

コマンドのモード

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。 • **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。

コマンドのモード

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

コマンド	説明
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。

コマンドのモード

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 ac
access-list ac; 2 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
```

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。

コマンドのモード

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 Version 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。

コマンドのモード

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。

コマンドのモード

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。

コマンドのモード

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。

コマンドのモード

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 7-2 に、各フィールドの説明を示します。

表 7-2　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 7-2　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。

コマンドのモード

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|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|
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|
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|
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|
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|
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|
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|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|
```

```
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|
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|
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|
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|
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|
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|
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|
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|
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。

コマンドのモード

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。

コマンドのモード

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。

コマンドのモード

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。

show asp drop

アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

show asp drop [**flow** *drop_reason* | **frame** *drop_reason*]

シンタックスの説明

flow	（オプション）ドロップされたフロー（接続）を表示します。
frame	（オプション）ドロップされたパケットを表示します。
drop_reason	（オプション）特定のプロセスによってドロップされたフローまたはパケットを表示します。ドロップ理由のリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show asp drop コマンドは、アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。この情報はデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

次のパケット ドロップ理由を指定すると、そのドロップ理由に関する統計情報を表示できます。

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

例

次に、**show asp drop** コマンドの出力例を示します。

```
hostname# show asp drop

Frame drop:
  Invalid encapsulation                                10897
  Invalid tcp length                                    9382
  Invalid udp length                                      10
  No valid adjacency                                    5594
  No route to host                                      1009
  Reverse-path verify failed                              15
  Flow is denied by access rule                       25247101
  First TCP packet not SYN                              36888
  Bad TCP flags                                         67148
  Bad option length in TCP                                731
  TCP MSS was too large                                 10942
  TCP Window scale on non-SYN                            2591
  Bad TCP SACK ALLOW option                               224
  TCP Dual open denied                                     11
  TCP data send after FIN                                  62
  TCP failed 3 way handshake                           328859
  TCP RST/FIN out of order                             258871
  TCP SEQ in SYN/SYNACK invalid                           142
  TCP ACK in SYNACK invalid                               278
  TCP packet SEQ past window                            46331
  TCP invalid ACK                                     1234749
  TCP packet buffer full                             90009943
  TCP RST/SYN in window                                 43136
  TCP DUP and has been ACKed                           927075
  TCP packet failed PAWS test                            9907
  Early security checks failed                              3
  Slowpath security checks failed                          19
  DNS Inspect invalid packet                             1097
  DNS Inspect invalid domain label                         10
  DNS Inspect packet too long                               5
  DNS Inspect id not matched                             8270
  FP L2 rule drop                                         783
  FP no mcast output intrf                                  5
  Interface is down                                      3881
  Non-IP packet received in routed mode                   158

Flow drop:
  Flow is denied by access rule                            24
  NAT failed                                            28739
  NAT reverse path failed                               22266
  Inspection failure                                    19433
```

関連コマンド

コマンド	説明
clear asp drop	アクセラレーション セキュリティ パスのドロップ統計情報を消去します。
show conn	接続に関する情報を表示します。

show asp table arp

アクセラレーション セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

シンタックスの説明

address *ip_address*	（オプション）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（オプション）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（オプション）IP アドレスのサブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show arp コマンドが制御プレーンの内容を表示するのに対して、**show asp table arp** コマンドはアクセラレーション セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

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

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

アクセラレーション セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類規則と対応付けます。それぞれの規則には、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。

show asp table classify [**crypto** | **domain** *domain_name* | **interface** *interface_name*]

シンタックスの説明

domain *domain_name*	（オプション）特定の分類子ドメインのエントリを表示します。ドメインのリストについては、「使用上のガイドライン」を参照してください。
interface *interface_name*	（オプション）分類子テーブルを表示する特定のインターフェイスを指定します。
crypto	（オプション）encrypt ドメイン、decrypt ドメイン、および ipsec-tunnel-flow ドメインのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show asp table classify コマンドは、アクセラレーション セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

分類子ドメインには、次のものがあります。

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
priority-q
punt
```

```
punt-l2
punt-root
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show asp table interfaces

アクセラレーション セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

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。

コマンドのモード

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

show asp table interfaces コマンドは、アクセラレーション セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
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。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show asp table mac-address-table

アクセラレーション セキュリティ パスの MAC アドレス テーブルをデバッグするには、特権 EXEC モードで **show asp table mac-address-table** コマンドを使用します。

show asp table mac-address-table [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）特定のインターフェイスの MAC アドレス テーブルを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show asp table mac-address-table コマンドは、アクセラレーション セキュリティ パスの MAC アドレス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table mac-address-table** コマンドの出力例を示します。

```
hostname# show asp table mac-address-table

interface                  mac  address       flags
-------------------------------------------------------
    inside1                     0009.b74d.3800     None
    inside1                     0007.e903.ad6e     None
    inside1                     0007.e950.2067     None
    inside1                     0050.0499.3749     None
    inside1                     0012.d96f.e200     None
    inside1                     0001.02a7.f4ec     None
    inside1                     0001.032c.6477     None
    inside1                     0004.5a2d.a1c8     None
    inside1                     0003.4773.c87b     None
    inside1                     000d.88ef.5d1c     None
    inside1                     00c0.b766.adce     None
    inside1                     0050.5640.450d     None
    inside1                     0001.03cf.0431     None
...
```

関連コマンド

コマンド	説明
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show asp table routing

アクセラレーション セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show asp table routing [**input** | **output**] [**address** *ip_address* [***netmask*** *mask*] | **interface** *interface_name*]

シンタックスの説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、サブネット マスクを含めることができます。スラッシュ（/）に続けて、プレフィックス（0 ～ 128）を入力します。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（オプション）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合に、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show asp table routing コマンドは、アクセラレーション セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

関連コマンド

コマンド	説明
show route	制御プレーン内のルーティング テーブルを表示します。

show asp table vpn-context

アクセラレーション セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

シンタックスの説明

detail	（オプション）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show asp table vpn-context コマンドは、アクセラレーション セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{***address*** *hex* | ***all*** | ***assigned*** | ***free*** | ***old*** | ***pool*** *size* [***summary***]} [**diagnostics** | ***dump*** | ***header*** | ***packet***] | ***queue history*** [***detail***]]

シンタックスの説明

address *hex*	（オプション）このアドレスに対応するブロックを 16 進形式で表示します。
all	（オプション）すべてのブロックを表示します。
assigned	（オプション）アプリケーションによって割り当てられ、使用されているブロックを表示します。
detail	（オプション）一意の各キュー タイプの最初のブロックの一部（128 バイト）を表示します。
dump	（オプション）ヘッダーとパケットの情報を含めて、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（オプション）ブロックに関する診断を表示します。
free	（オプション）使用可能なブロックを表示します。
header	（オプション）ブロックのヘッダーを表示します。
old	（オプション）1 分より前に割り当てられたブロックを表示します。
packet	（オプション）パケットの内容をブロックのヘッダーとともに表示します。
pool *size*	（オプション）特定のサイズのブロックを表示します。
queue history	（オプション）セキュリティ アプライアンスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。ブロックはプールから割り当てられますが、一度もキューに割り当てられないことがあります。この場合に表示される位置は、ブロックを割り当てたコードのアドレスです。
summary	（オプション）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	**pool summary** オプションが追加されました。

使用上のガイドライン

show blocks コマンドは、セキュリティ アプライアンスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックがセキュリティ アプライアンスを経由して移動している限り、メモリがすべて使用されている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが移動しているかどうかを確認できます。トラフィックが移動していないで、かつメモリがすべて使用されている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の最高水準点について、コンテキスト固有の情報とともにシステム全体の情報も含まれています。

表示される出力については、「例」の項を参照してください。

例

次に、シングルモードでの **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
SIZE    MAX    LOW    CNT
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

表 7-3 に、各フィールドの説明を示します。

表 7-3　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。下に例を示します。
4	DNS モジュール、ISAKMP モジュール、URL フィルタリング モジュール、uauth モジュール、TFTP モジュール、TCP モジュールなどのアプリケーションの既存ブロックを複製します。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。

表 7-3　show blocks のフィールド（続き）

フィールド	説明
256	ステートフル フェールオーバーのアップデート、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブなセキュリティ アプライアンスは、パケットを生成してスタンバイ セキュリティ アプライアンスに送信し、変換と接続のテーブルをアップデートします。接続が頻繁に作成または破棄されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイ セキュリティ アプライアンスに対してアップデートされなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、セキュリティ アプライアンスの処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態をセキュリティ アプライアンスが維持できない問題が発生しています。 セキュリティ アプライアンスから送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバに記録していないことを確認してください。この情報は、セキュリティ アプライアンス コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することをお勧めします。
1550	セキュリティ アプライアンスで処理するイーサネット パケットを格納するために使用されます。 パケットは、セキュリティ アプライアンス インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。セキュリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを出力インターフェイス上の出力キューに配置します。セキュリティ アプライアンスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT カラムに示されます）。CNT カラムが 0 になると、セキュリティ アプライアンスはさらにブロックを確保しようとします（最大で 8,192 個まで）。使用可能なブロックがなくなった場合、セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御アップデートに使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。ブロックの最大数は、ブートアップ時にメモリに基づいて配分されます。ブロックの最大数は、通常は変化しません。例外は 256 バイト ブロックと 1,550 バイト ブロックで、セキュリティ アプライアンスはこれらのブロックを必要に応じて動的に作成できます（最大で 8,192 個まで）。

表 7-3　show blocks のフィールド（続き）

フィールド	説明
LOW	最低水準点。この数は、セキュリティ アプライアンスの電源がオンになった時点、またはブロックの内容が（**clear blocks** コマンドで）最後に消去された時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがすべて使用されたことを示します。
CNT	指定したサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在すべて使用されていることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc
not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 7-4 に、各フィールドの説明を示します。

表 7-4　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。割り当て、取得、入力、解放の 4 つのいずれかです。
location	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

表 7-5 に、各フィールドの説明を示します。

表 7-5　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリで報告されなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されてコンテンツが無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられているメモリを増やします。
clear blocks	システム バッファの統計情報を消去します。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権コンフィギュレーション モードで ***show bootvar*** コマンドを使用します。

show bootvar

シンタックスの説明

show bootvar	システムのブート プロパティ。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
特権モード	•	•	•	•	•

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

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定するものです。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ ***boot system*** コマンドと ***boot config*** コマンドで設定します。

例

次の例では、BOOT 変数が disk0:/f1_image を保持しています。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:f1_backupimage です。これは、BOOT 変数が boot system コマンドで変更されているものの、実行コンフィギュレーションがまだ ***write memory*** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブート ローダーは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションをポイントします。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、***boot config*** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、***boot config*** コマンドで変更して、***write memory*** コマンドで保存することができます。

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show capture

キャプチャのコンフィギュレーションを表示するには、オプションを指定せずに **show capture** コマンドを使用します。

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** ***number***] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

シンタックスの説明

capture_name	（オプション）パケット キャプチャの名前。
access-list *access_list_name*	（オプション）特定のアクセスリストの IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
count *number*	（オプション）指定したパケットの数に関するデータを表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する isakmp データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。
detail	（オプション）各パケットの詳細なプロトコル情報を表示します。
dump	（オプション）データ リンク トランスポート経由で伝送されるパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

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。

コマンドのモード

セキュリティ コンテキスト モード: シングル コンテキスト モードおよびマルチ コンテキスト モード

アクセス場所：システムおよびコンテキストのコマンドライン

コマンド モード：特権モード

ファイアウォール モード : ルーテッド ファイアウォール モードおよび透過ファイアウォール モード

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

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC に関する情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって形式が異なります。表 7-6 で [ ] に囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 7-6　パケット キャプチャの出力形式

パケットのタイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*

表 7-6　パケット キャプチャの出力形式（続き）

パケットのタイプ	キャプチャの出力形式
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/ その他	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
その他	*HH:MM:SS.ms ether-hdr*: *hex-dump*

例

次の例は、キャプチャのコンフィギュレーションを表示する方法を示しています。

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次の例は、ARP キャプチャによってキャプチャされたパケットを表示する方法を示しています。

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

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。

コマンドのモード

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 chardrop** コマンドの出力例を示します。

```
hostname# show chardrop
```

Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0

関連コマンド

コマンド	説明
show running-config	現在の実行コンフィギュレーションを表示します。

show checkheaps

チェックヒープに関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ピープ メモリ バッファ（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられる）の健全性およびコード領域の完全性を確認する定期的なプロセスです。

show checkheaps

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。

コマンドのモード

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 checkheapls** コマンドの出力例を示します。

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	チェックヒープの確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

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。

コマンドのモード

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)	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 checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 16 進数の 4 つのグループを表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（セキュリティ アプライアンス フラッシュ パーティションからの読み込み、またはセキュリティ アプライアンス フラッシュ パーティションへの書き込み時）。「.」は、セキュリティ アプライアンスが処理に占有されているが「ハングアップ」していないことを示しています。このメッセージは、「system processing, please wait」メッセージと同様です。

例

次の例は、コンフィギュレーションまたはチェックサムを表示する方法を示しています。

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

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。

コマンドのモード

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

次の例は、チャンクに関する統計情報を表示する方法を示しています。

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show clock

セキュリティ アプライアンス上の時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

シンタックスの説明

detail	（オプション）クロックのソース（NTP またはユーザ設定）と現在のサマータイム設定（存在する場合）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。

コマンドのモード

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
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show clock** コマンドの出力例を示します。

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

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

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show conn [**all** | **count**] [**state** *state_type*] | [{{**foreign** | **local**} *ip* [*-ip2*] **netmask** *mask*}] | [**long** | ***detail***] | [{{**lport** | **fport**} *port1*} [*-port2*]] | [**protocol** {**tcp** | **udp**}]

シンタックスの説明

all	デバイスを通過するトラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（オプション）アクティブな接続の数を表示します。
detail	変換タイプとインターフェイスの情報を含めて、接続の詳細を表示します。
foreign	指定した外部 IP アドレスとの接続を表示します。
fport	指定した外部ポートとの接続を表示します。
ip	ドット付き 10 進表記の IP アドレス。または、IP アドレス範囲の開始アドレス。
-ip2	（オプション）IP アドレス範囲の終了 IP アドレス。
local	指定したローカル IP アドレスとの接続を表示します。
long	（オプション）接続をロング フォーマットで表示します。
lport	指定したローカル ポートとの接続を表示します。
netmask	指定した IP アドレスに使用するサブネット マスクを指定します。
mask	ドット付き 10 進表記のサブネット マスク。
port1	ポート番号。または、ポート番号範囲の開始ポート番号。
-port2	（オプション）ポート番号範囲の終了ポート番号。
protocol	（オプション）接続プロトコルを指定します。
state	（オプション）指定した接続の状態を表示します。
state_type	接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 7-7 を参照してください。
tcp	TCP プロトコル接続を表示します。
udp	UDP プロトコル接続を表示します。

コマンドのモード

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。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注） セカンダリ接続を可能にするためのピンホールをセキュリティ アプライアンスが作成するとき、この接続は **show conn** コマンドでは不完全な接続として表示されます。この不完全な接続を消去するには、**clear local** コマンドを使用します。

表 7-7 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。

表 7-7　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続。
conn_inbound	着信接続。
ctiqbe	CTIQBE 接続。
data_in	着信データ接続。
data_out	発信データ接続。
finin	FIN 着信接続。
finout	FIN 発信接続。
h225	H.225 接続。
h323	H.323 接続。
http_get	HTTP get 接続。
mgcp	MGCP 接続。
nojava	Java アプレットへのアクセスを拒否する接続。
rpc	RPC 接続。
sip	SIP 接続。
skinny	SCCP 接続。
smtp_data	SMTP メール データ接続。
sqlnet_fixup_data	SQL*Net データ検査エンジン接続。

detail オプションを使用すると、表 7-8 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

表 7-8　接続フラグ

フラグ	説明
a	SYN に対する外部 ACK（確認応答）を待機
A	SYN に対する内部 ACK（確認応答）を待機
B	外部からの初期 SYN
C	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）メディア接続
d	ダンプ
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN
g	Media Gateway Control Protocol（MGCP）接続
G	接続がグループの一部[1]
h	H.225
H	H.323
i	不完全な TCP または UDP 接続
I	着信データ

表 7-8　接続フラグ（続き）

フラグ	説明
k	Skinny Client Control Protocol（SCCP）メディア接続
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製（未使用）
P	内部バック接続
q	SQL*Net データ
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC[2]
s	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続[3]
T	SIP 接続[4]
U	アップ

1. G フラグは、接続がグループの一部であることを示します。GRE および FTP の Strict フィックスアップによって設定され、制御接続と関連するすべてのセカンダリ接続を指定します。制御接続が終了すると、関連するすべてのセカンダリ接続も終了します。
2. **show conn** コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
3. UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
4. UDP 接続の場合、値 T は、**timeout sip** コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。

（注）　DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS の識別情報は、*app_id* によって追跡され、各 app_id のアイドル タイマーはそれぞれ独立して動作します。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注）　**conn timeout** コマンドで定義した非アクティブ期間（デフォルトは 01:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

例

複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。次の例では、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示しています。

```
hostname# show conn state up,rpc,h323,sip
```

次の例は、内部ホスト 10.1.1.15 から 192.168.49.10 の外部 Telnet サーバへの TCP セッション接続を示しています。B フラグが存在しないため、接続は内部から開始されています。「U」フラグ、「I」フラグ、および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示しています。

```
hostname# show conn
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

次の例は、外部ホスト 192.168.49.10 から内部ホスト 10.1.1.15 への UDP 接続を示しています。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
hostname(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIBQE media, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, g - MGCP, H - H.323, h - H.255.0, I - inbound data, i - incomplete,
        k - Skinny media, M - SMTP data, m - SIP media
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
        s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

次に、**show conn all** コマンドの出力例を示します。

```
hostname# show conn all
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
  UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
  UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
  UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

例では、内部のホスト 10.3.3.4 が 209.165.201.1 の Web サイトにアクセスしています。外部インターフェイス上のグローバル アドレスは、209.165.201.7 です。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
inspect sip	Java アプレットを HTTP トラフィックから削除します。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

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。

コマンドのモード

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

次の例は、コンソール出力がない場合に表示されるメッセージを示しています。

```
hostname# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
show console-output	キャプチャされたコンソール出力を表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | ***detail*** | ***count***]

シンタックスの説明

count	（オプション）設定済みコンテキストの数を表示します。
detail	（オプション）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（オプション）コンテキスト名を設定します。名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。

コマンドのモード

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	このコマンドが導入されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show context** コマンドの出力例を示します。この表示例では、3 つのコンテキストが表示されています。

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 7-9 に、各フィールドの説明を示します。

表 7-9　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が一覧表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	コンテキストに割り当てられるインターフェイス。
URL	セキュリティ アプライアンスがコンテキストのコンフィギュレーションをロードする URL。

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

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 7-10 に、各フィールドの説明を示します。

表 7-10　コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
（状態メッセージ）	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。
Has been created, but initial ACL rules not complete	セキュリティ アプライアンスはコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、セキュリティ レベルの低い方から高い方に向かうトラフィックを拒否し、アプリケーション検査およびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックがセキュリティ アプライアンスを一切通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn’t been parsed	デフォルトの ACL がダウンロードされましたが、まだセキュリティ アプライアンスがコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、空白の実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。

表 7-10　コンテキストの状態（続き）

フィールド	説明
Real Interfaces	コンテキストに割り当てられるインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はインターフェイスの実際の名前を示しています。システム実行スペースは、すべてのインターフェイスを含んでいます。
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はマッピングされた名前を示しています。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

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

```
hostname# show context count
Total active contexts: 2
```

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。
allocate-interface	コンテキストにインターフェイスを割り当てます。
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。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | **context** *context-name* | **summary** | **top** *N* **]** [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

シンタックスの説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみ表示します。 範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。 範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

コマンドのモード

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

次の例は、すべてのカウンタを表示する方法を示しています。

```
hostname# show counters all
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   single_vf
IOS_IPC       OUT_PKTS              2   single_vf

hostname# show counters
Protocol      Counter           Value   Context
NPCP          IN_PKTS            7195   Summary
NPCP          OUT_PKTS           7603   Summary
IOS_IPC       IN_PKTS             869   Summary
IOS_IPC       OUT_PKTS            865   Summary
IP            IN_PKTS             380   Summary
IP            OUT_PKTS            411   Summary
IP            TO_ARP              105   Summary
IP            TO_UDP                9   Summary
UDP           IN_PKTS               9   Summary
UDP           DROP_NO_APP           9   Summary
FIXUP         IN_PKTS             202   Summary
```

次の例は、カウンタの要約を表示する方法を示しています。

```
hostname# show counters summary
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   Summary
IOS_IPC       OUT_PKTS              2   Summary
```

次の例は、コンテキストのカウンタを表示する方法を示しています。

```
hostname# show counters context single_vf
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               4   single_vf
IOS_IPC       OUT_PKTS              4   single_vf
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu usage** コマンドを使用します。

show cpu [**usage**]

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

show cpu [**usage**] [**context** {**all** | *context_name*}]

シンタックスの説明

all	すべてのコンテキストを表示の対象にすることを指定します。
context	1 つのコンテキストを表示の対象にすることを指定します。
context_name	表示の対象にするコンテキストの名前を指定します。
usage	（オプション）CPU 使用状況を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

CPU の使用状況は、負荷の近似値を使用して 5 秒ごとに算出されます。この近似値は、次回と次々回の移動平均に提供されます。

show cpu コマンドを使用すると、負荷に関係しているプロセス（つまり、シングルモードで実行した ***show process*** コマンドと、マルチ コンテキスト モードのシステム コンフィギュレーションから実行した ***show process*** コマンドの両方の出力に表示されている項目のためのアクティビティ）を発見できます。

さらに、マルチ コンテキスト モードでは、いずれかの設定済みコンテキストが CPU に負荷をかけている場合、その負荷に関係しているプロセスを中断するように要求できます。このためには、各コンテキストに移動して ***show cpu*** コマンドを入力するか、このコマンドの変化型である ***show cpu context*** を入力します。

プロセスに関係する負荷は、直近の整数に四捨五入されます。それに対して、コンテキストに関係する負荷には小数点第 1 位が含まれています。たとえば、***show cpu*** をシステム コンテキストから入力すると、***show cpu context system*** コマンドを入力したときとは別の数値が示されます。前者は ***show cpu context all*** のすべての要素の近似的な要約であり、後者はその要約の一部にすぎません。

例

次の例は、CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次の例は、マルチ モードでシステム コンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次の例は、すべてのコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次の例は、one というコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

show crashinfo

フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示するには、特権 EXEC モードで ***show crashinfo*** コマンドを入力します。

show crashinfo [**save**]

シンタックスの説明

save	（オプション）クラッシュ情報をフラッシュ メモリに保存するようにセキュリティ アプライアンスが設定されているかどうかを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンドで生成）のものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Test_Crash**」であり、最後の文字列は「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュのものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Crash**」であり、最後の文字列は「**: End_Crash**」です（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データを消去していた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

例

次の例は、現在のクラッシュ情報コンフィギュレーションを表示する方法を示しています。

```
hostname# show crashinfo save
crashinfo save enable
```

次の例は、クラッシュ ファイル テストの出力を示しています（このテストによって、セキュリティ アプライアンスが実際にクラッシュすることはありません。このテストで生成されるのは、擬似的なサンプル ファイルです）。

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
```

```
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
```

```
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
```

```
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------
```

```
0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


     PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
```

```
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。

show crashinfo console

フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行うには、**crashinfo console disable** コマンドを使用します。このコマンドは、クラッシュを強制的に発生させます。

show crashinfo console

シンタックスの説明

console	クラッシュ情報をコンソールに出力するかどうかを制御します。

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。

コマンドのモード

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(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 140-2 に準拠すると、キーやパスワードなどのクリティカル セキュリティ パラメータを暗号境界（シャーシ）の外側に配布することができません。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域は、機密データを含んでいることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

show crypto accelerator statistics

ハードウェア暗号アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、グローバルな暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
```

```
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                              Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                              SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                              IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにインストールされているすべての証明書が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	•	—
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

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CA 証明書を表示しています。

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ca crls

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにキャッシュされているすべての CRL が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	•	
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

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CRL を表示しています。

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットの IPSec DF ビット ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

シンタックスの説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

次の例では、inside というインターフェイスの IPSec DF ビット ポリシーを表示しています。

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

シンタックスの説明

interface	インターフェイス名を指定します。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、inside というインターフェイスの IPSec フラグメンテーション ポリシーを表示しています。

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto key mypubkey

指定したタイプのキー ペアを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto key mypubkey** コマンドを使用します。

show crypto key mypubkey {***rsa*** | ***dsa***}

シンタックスの説明

dsa	DSA キー ペアを表示します。
rsa	RSA キー ペアを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、RSA キー ペアを表示しています。

```
hostname(config)# show crypto key mypubkey rsa
[Display]
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key generate dsa	DSA キー ペアを生成します。
crypto key generate rsa	RSA キー ペアを生成します。
crypto key zeroize	指定したタイプのすべてのキー ペアを削除します。

show crypto protocol statistics

暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を表示するプロトコルの名前を指定します。指定できるプロトコルは、次のとおりです。 ***ikev1***：Internet Key Exchange バージョン 1 ***ipsec***：IP セキュリティ フェーズ 2 プロトコル ***ssl***：Secure Socket Layer ***other***：新しいプロトコルのために予約済み ***all***：現在サポートされているすべてのプロトコル

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、指定したプロトコルに関する暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0
```

```
hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
```

```
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。

show ctiqbe

セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

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。

コマンドのモード

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。

使用上のガイドライン

show ctiqbe コマンドは、セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** と共に、このコマンドは、CTIQBE 検査エンジンの問題のトラブルシューティングに使用されます。

（注）　**show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンスを越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco Call Manager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# show ctiqbe

Total: 1
  LOCAL  FOREIGN  STATE  HEARTBEAT
------------------------------------------------------------
1  10.0.0.99/1117   172.29.1.77/2748  1  120
  RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028  1029)
  MEDIA: Device ID 27  Call ID 0
  Foreign 172.29.1.99  (1028  1029)
  Local  172.29.1.88  (26822  26823)
  ---------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスと RTP リスン ポートは、172.29.1.99 UDP ポート 1028 に PAT 変換されています。その RTCP リスン ポートは、UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートは、その外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP リスン ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

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。

コマンドのモード

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	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように修正されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次の例は、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力を示しています。ユーザ名はログイン時にユーザが入力した名前を示し、P_PRIV はユーザが **enable** コマンドを入力したことを示し、P_CONF は **config terminal** コマンドを入力したことを示します。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
show running-config privilege	コマンドの特権レベルを表示します。

show debug

現在のデバッグ コンフィギュレーションを表示するには、**show debug** コマンドを使用します。

show debug [*command* [*keywords*]]

シンタックスの説明

command	（オプション）現在のコンフィギュレーションを表示するデバッグ コマンドを指定します。*command* 以降のシンタックスは、各 *command* の関連 **debug** コマンドでサポートされているシンタックスと同じです。たとえば、**show debug aaa** 以降で有効となる *keywords* は、**debug aaa** コマンドで有効となるキーワードと同じです。つまり、**show debug *aaa*** の場合は ***accounting*** キーワードをサポートしています。このキーワードを使用すると、AAA デバッグの当該部分のデバッグ コンフィギュレーションを表示することを指定できます。

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。

コマンドのモード

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。

使用上のガイドライン

有効となる *command* 値は、次のとおりです。*command* 以降で有効となるシンタックスについては、該当する **debug** *command* のエントリを参照してください。

（注）　それぞれの *command* 値を入力できるかどうかは、該当する **debug** コマンドをサポートしているコマンド モードによって異なります。

- **aaa**
- **appfw**

- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**

- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**

例

次のコマンドでは、認証、アカウンティング、およびフラッシュ メモリについてデバッグをイネーブルにしています。**show debug** コマンドを 3 つの方法で使用して、すべてのデバッグ コンフィギュレーション、特定の機能のデバッグ コンフィギュレーション、および機能のサブセットのデバッグ コンフィギュレーションを表示する方法を示しています。

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
debug	すべての **debug** コマンドを参照してください。

show dhcpd

DHCP のバインディング、状態、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcpd** コマンドを使用します。

show dhcpd {***binding*** [*IP_address*] | ***state*** | ***statistics***}

シンタックスの説明

binding	与えられたサーバの IP アドレスとそれに関連付けられているクライアント ハードウェア アドレスとリース期間に対するバインディング情報を表示します。
IP_address	指定した IP アドレスのバインディング情報を表示します。
state	DHCP サーバの状態を表示します。たとえば、現在のコンテキストでイネーブルになっているかどうか、各インターフェイスでイネーブルになっているかどうかなどです。
statistics	アドレス プール、バインディング、有効期限切れのバインディング、形式が誤っているメッセージ、送信済みメッセージ、および受信済みメッセージの数などの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show dhcpd binding コマンドにオプションの IP アドレスを含めると、その IP アドレスのバインディングのみが表示されます。

show dhcpd binding | state | statistics コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

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

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

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

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

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

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools         1
Automatic bindings    1
Expired bindings      1
Malformed messages    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          1
DHCPREQUEST           2
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             1
DHCPACK               1
DHCPNAK               1
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
clear dhcpd	DHCP サーバのバインディングおよび統計情報カウンタをクリアします。
dhcpd lease	クライアントに与える DHCP 情報のリース期間を定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

show dhcprelay state

DHCP リレー エージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

show dhcprelay state

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。

コマンドのモード

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。

使用上のガイドライン

このコマンドは、現在のコンテキストおよび各インターフェイスの DHCP リレー エージェントの状態情報を表示します。

例

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

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

関連コマンド

コマンド	説明
show dhcpd	DHCP サーバの統計情報と状態情報を表示します。
show dhcprelay statistics	DHCP リレーの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

show dhcprelay ***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。

コマンドのモード

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。

使用上のガイドライン

show dhcprelay statistics コマンドの出力は、**clear dhcprelay satistics** コマンドを入力するまでは増分します。

例

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

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay state	DHCP リレー エージェントの状態を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

show disk

フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show disk** コマンドを使用します。PIX セキュリティ アプライアンスのフラッシュ メモリを表示するには、**show flash** コマンドを参照してください。

show disk[**0** | **1**] [**filesys** | **all**]

シンタックスの説明

0	**1**	内部フラッシュ メモリ（0。デフォルト）または外部フラッシュメモリ（1）を指定します。
filesys	コンパクト フラッシュ カードに関する情報を表示します。
all	フラッシュ メモリの内容に加えてファイル システム情報を表示します。

デフォルト

デフォルトでは、内部フラッシュ メモリが表示されます。

コマンドのモード

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	このコマンドが導入されました。

例

次に、**show disk** コマンドの出力例を示します。

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

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

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show flash	内部フラッシュ メモリの内容を表示します。

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバから動的にラーニングしたエントリとともに、**name** コマンドを使用して手作業で入力した名前および IP アドレスが保持されています。

show dns-hosts

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。

コマンドのモード

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

表示される出力については、「例」の項を参照してください。

例

次に、**show dns-hosts** コマンドの出力例を示します。

```
hostname# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

表 7-11 に、各フィールドの説明を示します。

表 7-11　show dns-hosts のフィールド

フィールド	説明
Host	ホスト名を表示します。
Flags	次のフラグを組み合せて、エントリのステータスを表示します。 • temp：このエントリは、DNS サーバから取得した一時的なものです。セキュリティ アプライアンスは、非アクティブ状態が 72 時間を過ぎるとこのエントリを削除します。 • perm：このエントリは、**name** コマンドで追加された永続的なものです。 • OK：このエントリは有効です。 • ??：このエントリは問題のある可能性があり、再確認が必要です。 • EX：このエントリは、有効期限が切れています。
Age	このエントリが最後に参照された時点からの経過時間を表示します。
Type	DNS レコードのタイプを表示します。この値は、常に IP です。
Address(es)	IP アドレス。

関連コマンド

コマンド	説明
clear dns-hosts cache	DNS キャッシュをクリアします。
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受け取らなかった場合に、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。

show failover

装置のフェールオーバー ステータスに関する情報を表示するには、特権 EXEC モードで **show failover** コマンドを使用します。

show failover [***group*** *num* | ***history*** | ***interface*** | ***state*** | ***statistics***]

シンタックスの説明

group	指定したフェールオーバー グループの動作状態を表示します。
history	フェールオーバーの履歴を表示します。フェールオーバーの履歴には、過去のフェールオーバーの状態変化、および状態変化の理由が表示されます。
interface	フェールオーバー コマンドとステートフル リンクの情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー装置のフェールオーバー状態を表示します。表示される情報には、装置がプライマリとセカンダリのどちらであるか、アクティブとスタンバイのどちらであるかというステータス情報が含まれ、装置が障害状態になっている場合は障害の理由も含まれています。
statistics	フェールオーバー コマンド インターフェイスの送信パケットと受信パケットの数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	このコマンドが変更されました。出力に含まれる情報を追加しています。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバーの情報、インターフェイスのステータス、およびステートフル フェールオーバーの統計情報を表示します。Stateful Failover Logical Update Statistics の出力は、ステートフル フェールオーバーがイネーブルになっている場合のみ表示されます。「xerrs」値および「rerr」値は、フェールオーバーにおけるエラーは指摘しませんが、むしろ、パケット送信または受信のエラーの数を示します。

show failover コマンドの出力で、各フィールドに表示される値は次のとおりです。

- Stateful Obj には、次の値が表示されます。
  - xmit：送信したパケット数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケット数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定オブジェクトのスタティック カウント用です。
  - General：ステートフル オブジェクト全部の合計を示します。
  - sys cmd：論理アップデート システム コマンド、たとえば、**login** または **stay alive** を参照します。
  - up time：アクティブ セキュリティ アプライアンスがスタンバイ セキュリティ アプライアンスに渡すアップタイムの値を示します。
  - RPC services：リモート プロシージャ コール接続の情報。
  - TCP conn：ダイナミック TCP 接続の情報。
  - UDP conn：ダイナミック UDP 接続の情報。
  - ARP tbl：ダイナミック ARP テーブルの情報。
  - Xlate_Timeout：接続変換タイムアウトの情報を示します。
  - VPN IKE upd：IKE 接続の情報。
  - VPN IPSEC upd：IPSec 接続の情報。
  - VPN CTCP upd：cTCP トンネル接続の情報。
  - VPN SDI upd：SDI AAA 接続の情報。
  - VPN DHCP upd：トンネリングされた DHCP 接続の情報。

フェールオーバー IP アドレスを入力していなければ、**show failover** コマンドは IP アドレスに対して 0.0.0.0 を表示し、インターフェイスのモニタリングは、「waiting」状態のままになります。フェールオーバーが動作するためには、フェールオーバー IP アドレスを設定する必要があります。

マルチ コンフィギュレーション モードでは、セキュリティ コンテキストで使用できるのは **show failover** コマンドのみです。オプションのキーワードは入力できません。

例

次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                Interface inside (10.130.9.3): Normal
                Interface outside (10.132.9.3): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                Interface inside (10.130.9.4): Normal
                Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

次に、Active/Active フェールオーバーでの **show failover** コマンドの出力例を示します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

関連コマンド

コマンド	説明
show running-config failover	現在のコンフィギュレーション内の **failover** コマンドを表示します。

show file

ファイル システムに関する情報を表示するには、特権 EXEC モードで **show file** コマンドを使用します。

show file descriptors | system | information *filename*

シンタックスの説明

descriptors	開かれているファイル記述子をすべて表示します。
information	特定のファイルに関する情報を表示します。
filename	ファイル名を指定します。
system	ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

次の例は、ファイル システムに関する情報を表示する方法を示しています。

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)     Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
pwd	現在の作業ディレクトリを表示します。

show firewall

現在のファイアウォール モード（ルーテッドまたは透過）を表示するには、特権 EXEC モードで **show firewall** コマンドを使用します。

show firewall

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。

コマンドのモード

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 firewall** コマンドの出力例を示します。

```
hostname# show firewall
Firewall mode: Router
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを設定します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

show flash

内部フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show flash:** コマンドを使用します。

show flash:

（注）　ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

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。

コマンドのモード

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

次の例は、内部フラッシュ メモリの内容を表示する方法を示しています。

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show disk0	内部フラッシュ メモリの内容を表示します。
show disk1	外部フラッシュ メモリ カードの内容を表示します。

show fragment

IP フラグメント再構成モジュールの運用データを表示するには、特権 EXEC モードで ***show fragment*** コマンドを入力します。

show fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンドのモード

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
イネーブル EXEC モード	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	コンフィギュレーション データを運用データから分離するために、コマンドが ***show fragment*** と ***show running-config fragment*** の 2 つのコマンドに分割されました。

例

次の例は、IP フラグメント再構成モジュールの運用データを表示する方法を示しています。

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションを消去し、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show gc

ガーベッジ コレクション プロセスに関する統計情報を表示するには、特権 EXEC モードで **show gc** コマンドを使用します。

show gc

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。

コマンドのモード

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 gc** コマンドの出力例を示します。

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :           0
Total udp conn delete response             :           0
Total number of zombie cleaned             :           0
Total number of embryonic conn cleaned     :           0
Total error response                       :           0
Total queries generated                    :           0
Total queries with conn present response   :           0
Total number of sweeps                     :         946
Total number of invalid vcid               :           0
Total number of zombie vcid                :           0
```

関連コマンド

コマンド	説明
clear gc	ガーベッジ コレクション プロセスに関する統計情報を削除します。

show h225

セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示するには、特権 EXEC モードで **show h225** コマンドを使用します。

show h225

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。

コマンドのモード

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。

使用上のガイドライン

show h225 コマンドは、セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示します。**debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

show h225、**show h245**、または **show h323-ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。多くのセッション レコードが存在し、**pager** コマンドが設定されていない場合、**show** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値を基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

例

次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
  Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
  1. CRV 9861
  Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
  Local: 10.130.56.4/1050 Foreign: 172.30.254.205/1720
```

この出力は、現在セキュリティ アプライアンスを通過しているアクティブ H.323 コールが 1 つ、ローカル エンドポイント 10.130.56.3 と外部のホスト 172.30.254.203 の間にあることを示しています。また、これらの特定のエンドポイントの間に、同時コールが 1 つあり、そのコールの CRV（Call Reference Value）が 9861 であることを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続に許容されるアイドル時間で、経過後にその接続が終了します。

show h245

スロー スタートを使用しているエンドポイントによって、セキュリティ アプライアンスを越えて確立されている H.245 セッションの情報を表示するには、特権 EXEC モードで **show h245** コマンドを使用します。

show h245

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。

コマンドのモード

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。

使用上のガイドライン

show h245 コマンドは、スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します（スロースタートは、コールの 2 つのエンドポイントが H.245 用の別の TCP コントロール チャネルを開いた場合です。ファースト スタートは、H.245 メッセージが H.225 コントロール チャネル上の H.225 メッセージの一部として交換された場合です）。**debug h323 h245 event**、**debug h323 h225 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

例

次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

セキュリティ アプライアンスを越えているアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します（TKTP ヘッダーは、各 H.225/H.245 メッセージの前に送られる 4 バイトのヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さが分かります）。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされたメディアには、258 という LCN（論理チャネル番号）があり、外部に 172.30.254.203/49608 という RTP IP アドレス / ポート ペアと 172.30.254.203/49609 という RTCP IP アドレス / ポート ペアを持ち、ローカルに 10.130.56.3/49608 という RTP IP アドレス / ポート ペアと 49609 という RTCP ポートを持っています。

259 という 2 番目の LCN には、外部に 172.30.254.203/49606 という RTP IP アドレス / ポート ペアと 172.30.254.203/49607 という RTCP IP アドレス / ポート ペアがあり、ローカルに 10.130.56.3/49606 という RTP IP アドレス / ポート ペアと 49607 という RTCP ポートを持っています。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続に許容されるアイドル時間で、経過後にその接続が終了します。

show h323-ras

ゲートキーパーとその H.323 エンドポイントの間でセキュリティ アプライアンスを越えて確立されている H.323 RAS セッションの情報を表示するには、特権 EXEC モードで **show h323-ras** コマンドを使用します。

show h323-ras

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。

コマンドのモード

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。

使用上のガイドライン

show h323-ras コマンドは、セキュリティ アプライアンスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。**debug h323 ras event** および **show local-host** コマンドと共に、このコマンドは、H.323 RAS 検査エンジンの問題のトラブルシューティングに使用されます。

show h323-ras コマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用される接続情報を表示します。詳細については、**inspect protocol h323 {h225 | ras}** コマンドのページを参照してください。

例

次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
|GK|Caller
|172.30.254.214 10.130.56.14
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続に許容されるアイドル時間で、経過後にその接続が終了します。

show history

以前に入力したコマンドを表示するには、ユーザ EXEC モードで **show history** コマンドを使用します。

show history

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。

コマンドのモード　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
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show history** コマンドを使用すると、以前に入力したコマンドを表示できます。上矢印キーと下矢印キーを使用したり、**^p** を入力して入力済みの行を表示したり、**^n** を入力して次の行を表示したりして、コマンドを個々に調べることができます。

例　次の例は、以前に入力したコマンドをユーザ EXEC モードに入っているときに表示する方法を示しています。

```
hostname> show history
    show history
    help
    show history
```

次の例は、以前に入力したコマンドを特権 EXEC モードに入っているときに表示する方法を示しています。

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

次の例は、以前に入力したコマンドをグローバル コンフィギュレーション モードに入っているときに表示する方法を示しています。

```
hostname(config)# show history
    show history
    help
    show history
    enable
    show history
    config t
    show history
```

関連コマンド

コマンド	説明
help	指定したコマンドのヘルプを表示します。

show icmp

ICMP コンフィギュレーションを表示するには、特権 EXEC モードで **show icmp** コマンドを使用します。

show icmp

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show icmp コマンドは、ICMP コンフィギュレーションを表示します。

例

次の例では、ICMP コンフィギュレーションを表示しています。

```
hostname# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
inspect icmp	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

インターフェイス記述子ブロックのステータスに関する情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

show idb

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。

コマンドのモード

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
ユーザ 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

IDB は、インターフェイスのリソースを表現するための内部データ構造です。表示される出力については、「例」の項を参照してください。

例

次に、**show idb** コマンドの出力例を示します。

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
              Active 6          21
            Inactive 1          2
          Total IDBs 7          23
 Size each (bytes) 116          212
        Total bytes 812         4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
```

```
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

表 7-12 に、各フィールドの説明を示します。

表 7-12　show idb stats のフィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システムのハードウェア ポートごとに作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システムのメイン インターフェイスとサブインターフェイスごと、およびコンテキストに割り当てられているインターフェイスごとに作成されます。 他の一部の内部ソフトウェア モジュールも IDB を作成します。
HWIDB#	ハードウェア インターフェイスのエントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェア インターフェイスのエントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

関連コマンド

コマンド	説明
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。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show igmp groups

セキュリティ アプライアンスに直接接続し、IGMP によってラーニングされたレシーバーがあるマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

show igmp groups [[***reserved*** | *group*] [*if_name*] [***detail***]] | ***summary***]

シンタックスの説明

detail	（オプション）送信元の詳細な説明を表示します。
group	（オプション）IGMP グループのアドレス。このオプション引数を指定すると、表示される情報は指定したグループに関するものだけになります。
if_name	（オプション）指定したインターフェイスのグループ情報を表示します。
reserved	（オプション）予約済みグループに関する情報を表示します。
summary	（オプション）グループ加入の要約情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

オプションの引数とキーワードをすべて省略した場合、**show igmp groups** コマンドは、直接接続しているすべてのマルチキャスト グループをグループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

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

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

show igmp interface

インターフェイスのマルチキャスト情報を表示するには、特権 EXEC モードで **show igmp interface** コマンドを使用します。

show igmp ***interface*** [*if_name*]

シンタックスの説明

if_name	（オプション）選択したインターフェイスの IGMP グループ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	このコマンドが変更されました。***detail*** キーワードが削除されました。

使用上のガイドライン

オプションの *if_name* 引数を省略した場合、**show igmp interface** コマンドはすべてのインターフェイスの情報を表示します。

例

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

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続される受信者を保持していて、IGMP を通じてラーニングされたマルチキャスト グループを表示します。

show igmp traffic

IGMP トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show igmp traffic** コマンドを使用します。

show igmp traffic

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。

コマンドのモード

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 igmp traffic** コマンドの出力例を示します。

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP 統計情報カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

show interface

インターフェイスに関する統計情報を表示するには、ユーザ EXEC モードで **show interface** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] [***stats*** | ***detail***]

シンタックスの説明

detail	（オプション）インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態が含まれ、非対称ルーティングが **asr-group** コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。すべてのインターフェイスを表示する場合、SSM 用の内部インターフェイスが ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
stats	（デフォルト）インターフェイスに関する情報と統計情報を表示します。このキーワードはデフォルトであるため、入力を省略できます。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

オプションを指定しない場合は、すべてのインターフェイスに関する基本的な統計情報が表示されます。

コマンドのモード

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
ユーザ EXEC	•	•	•	•	•

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、新しいインターフェイス番号付け方式を取り入れるように修正され、明示的な指定をするための ***stats*** キーワード、および ***detail*** キーワードが追加されました。
7.0(4)	このコマンドに 4GE SSM インターフェイスのサポートが追加されました。

使用上のガイドライン

インターフェイスが複数のコンテキストで共有されている場合は、コンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストに関する統計情報のみ表示します。このコマンドをシステム実行スペースで物理インターフェイスに関して入力すると、セキュリティ アプライアンスはすべてのコンテキストの合算統計情報を表示します。

サブインターフェイスに関して表示される統計情報の数は、物理インターフェイスに関して表示される統計情報の数のサブセットです。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。**allocate-interface** コマンドで ***visible*** キーワードを設定した場合、セキュリティ アプライアンスは **show interface** コマンドの出力にインターフェイスの ID を表示します。

表示される出力については、「例」の項を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
hostname> show interface
Interface GigabitEthernet0/0 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 000f.f775.540e, MTU not set
        IP address unassigned
        752 packets input, 173435 bytes, 0 no buffer
        Received 752 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        752 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/6) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
Interface Management0/0 "intm00", is up, line protocol is up
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 000f.f775.5412, MTU 1500
        IP address unassigned
        751 packets input, 170487 bytes, 0 no buffer
        Received 753 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/1)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 738 VLAN untagged packets, 156831 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 413 VLAN untagged packets
        Management-only interface. Blocked 0 through-the-device packets
                0 IPv4 packets originated from management network
                0 IPv4 packets destined to management network
                0 IPv6 packets originated from management network
                0 IPv6 packets destined to management network
```

```
Interface GigabitEthernet1/0 "intg10", is down, line protocol is down
  Hardware is VCS7380 rev01, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Media-type configured as RJ45 connector
        MAC address 000b.fcff.b548, MTU 1500
        IP address 17.1.9.115, subnet mask 255.0.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 rate limit drops
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 0 VLAN untagged packets, 0 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 0 VLAN untagged packets
...
```

表 7-13 に、各フィールドの説明を示します。

表 7-13　show interface のフィールド

フィールド	説明
Interface *ID*	インターフェイス ID。コンテキスト内では、**allocate-interface** コマンドで ***visible*** キーワードを設定しない限り、セキュリティ アプライアンスはマッピング名（設定されている場合）を表示します。
“*interface_name*”	**nameif** コマンドで設定したインターフェイス名。システム内でこの名前を設定することはできないため、システム実行スペースでは、このフィールドは空白です。名前を設定していない場合は、Hardware 行の後に次のメッセージが表示されます。 `Available but not configured via nameif`
is *state*	管理状態。次のいずれかです。 • up：インターフェイスはシャットダウンされていません。 • administratively down：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Line protocol is *state*	回線の状態。次のいずれかです。 • up：使用しているケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが誤っているか、インターフェイス コネクタに接続されていません。
VLAN identifier	サブインターフェイスの VLAN ID。
Hardware	インターフェイスのタイプ、最大帯域幅、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコ（）で囲まれて設定値とともに表示されます。
Media-type	（4GE SSM インターフェイスのみ）インターフェイスが RJ-45 または SFP のいずれとして設定されているかを表示します。

表 7-13　show interface のフィールド（続き）

フィールド	説明

message area	特定の状況下で、メッセージが表示されることがあります。次の例を参照してください。
	• システム実行スペースでは、次のメッセージが表示されることがあります。
	`Available for allocation to a context`
	• 名前を設定していない場合は、次のメッセージが表示されます。
	`Available but not configured via nameif`

MAC address	インターフェイスの MAC アドレス。
MTU	このインターフェイスで許容されるパケットの最大サイズ（バイト単位）。インターフェイス名を設定していない場合、このフィールドには「MTU not set」と表示されます。
IP address	**ip address** コマンドを使用して設定した、または DHCP サーバから受信したインターフェイス IP アドレス。システム内で IP アドレスを設定することはできないため、システム実行スペースでは、このフィールドに「IP address unassigned」と表示されます。
Subnet mask	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信されたパケット数。
Bytes	このインターフェイスで受信されたバイト数。
No buffer	メイン システムのバッファ スペースがなかったために、廃棄された受信済みパケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
Received:	
Broadcasts	受信されたブロードキャストの数。
Runts	最小限のパケット サイズ（64 バイト）よりも小さいために廃棄されたパケットの数。ラントの原因は、通常は衝突です。不適切な配線や電気干渉が原因となって発生することもあります。
Giants	最大パケット サイズを超えているために廃棄されたパケットの数。たとえば、1,518 バイトを超えるイーサネット パケットはすべてジャイアントと見なされます。
Input errors	下に示したタイプを含めた、入力エラーの総数。入力に関係しているこの他のエラーも、入力エラーの数が増加する原因になります。また、一部のデータグラムは複数のエラーを包含していることもあります。したがって、この合計数は下に示したタイプについて表示されるエラーの数を超える場合があります。
CRC	巡回冗長検査エラーの数。ステーションは、フレームを送信するときにフレーム末尾に CRC を付加します。この CRC は、フレームに含まれているデータに基づいて、アルゴリズムに従って生成されます。送信元と宛先の中間でフレームが改変された場合、セキュリティ アプライアンスは、CRC が一致しないことを指摘します。CRC の値が大きくなる原因は、通常は衝突か、不良データを転送しているステーションです。

表 7-13　show interface のフィールド（続き）

フィールド	説明
Frame	フレーム エラーの数。不良フレームには、長さが不適切なパケット、またはフレーム チェックサムの正しくないパケットが含まれています。このエラーが発生する原因は、通常は衝突か、故障しているイーサネット デバイスです。
Overrun	入力レートがセキュリティ アプライアンスのデータ処理能力を超えたために、受信したデータをセキュリティ アプライアンスがハードウェア バッファに渡すことができなかった回数。
Ignored	インターフェイス ハードウェアの内部バッファが不足したために、インターフェイスによって無視された受信パケットの数。これらのバッファは、バッファの説明で前に述べたシステム バッファとは別のものです。無視される数は、ブロードキャスト ストームとバースト雑音が原因となって増加する場合もあります。
Abort	このフィールドは使用されません。この値は常に 0 です。
L2 decode drops	名前が（**nameif** コマンドで）設定されていないため、または無効な VLAN ID を持つフレームを受信したために、ドロップされたパケットの数。
Packets output	このインターフェイスで送信されたパケット数。
Bytes	このインターフェイスで送信されたバイト数。
Underruns	トランスミッタの動作速度がセキュリティ アプライアンスの処理速度を上回った回数。
Output Errors	衝突が設定されている最大数を超えたために伝送されなかったフレーム数。このカウンタは、ネットワーク トラフィックが大きい間は増加します。
Collisions	イーサネット衝突（1 つまたは複数の衝突）が原因で、再送されたメッセージ数。これは、通常、拡張しすぎた LAN（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間にリピータが 3 つ以上ある、またはカスケード接続されたマルチポート トランシーバが多すぎる）で発生します。衝突したパケットは、出力パケットによって一度だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスが 3 秒間伝送できない場合、セキュリティ アプライアンスはインターフェイスをリセットして、伝送を再開します。この間隔の間も、接続状態は保持されます。インターフェイスのリセットは、インターフェイスがループバックされた場合、またはシャットダウンされた場合にも起こります。
Babbles	未使用。「babble」は、トランスミッタがインターフェイス上に留まっている時間が、最大長のフレームの伝送に要する時間を超えたことを意味します。

表 7-13　show interface のフィールド（続き）

フィールド	説明
Late collisions	衝突が表示される通常のウィンドウに表示されない衝突が発生したために伝送されなかったフレーム数。遅延衝突は、パケットの伝送で遅れて検出される衝突です。通常は、このようなことは起こらないようになっています。2 つのイーサネット ホストが同時に伝送を試みた場合、両ホストが早期にパケットの衝突を起こして両方がバックオフするか、2 番目のホストが 1 番目のホストの伝送に気付いて待機します。 遅延衝突が発生した場合、デバイスが割り込んでイーサネット上でパケットの送信を試み、同時にセキュリティ アプライアンスがパケットの送信を一部終了します。セキュリティ アプライアンスは、パケットの最初の部分が入ったバッファをすでに解放してしまっている可能性があるため、パケットを再送信しません。ネットワーキング プロトコルは、パケットを再送信することで衝突に対処するように設計されているため、これは大きな問題ではありません。しかし、遅延衝突はネットワークに問題が存在することを示します。よくある問題は、リピータを何台も使用して拡張したネットワーク、および仕様範囲外で動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で、伝送前に延期されたフレーム数。
Rate limit drops	（4GE SSM インターフェイスのみ）転送速度がギガビットではないインターフェイスを設定して、10Mbps を超える速度で転送しようとした場合に、ドロップされたパケットの数。
Lost carrier	伝送中に搬送信号が消失した回数。
No carrier	未使用。
Input queue (curr/max blocks):	入力キューに入っているパケットの数（現在値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Output queue (curr/max blocks):	出力キューに入っているパケットの数（現在値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Received [VLAN untagged] packets	物理インターフェイスの場合は、タグの付いていない受信済み VLAN パケットの数とバイト数。 サブインターフェイスの場合は、適切な VLAN を使用してタグが付けられた受信済みパケットの数。
Transmitted [VLAN untagged] packets	物理インターフェイスの場合は、タグの付いていない送信済み VLAN パケットの数とバイト数。 サブインターフェイスの場合は、適切な VLAN を使用してタグが付けられた送信済みパケットの数。
Dropped [VLAN untagged] packets	物理インターフェイスの場合は、タグの付いていないドロップ済み VLAN パケットの数。 サブインターフェイスの場合は、適切な VLAN を使用してタグが付けられたドロップ済みパケットの数。

次に、**show interface detail** コマンドの出力例を示します。次の例では、すべてのインターフェイスに関する詳細なインターフェイス統計情報を表示しています。この情報には、内部インターフェイス（プラットフォームに存在する場合）が含まれ、非対称ルーティングが **asr-group** コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。

```
hostname> show interface detail
Interface GigabitEthernet0/0 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 000f.f775.540e, MTU not set
        IP address unassigned
        752 packets input, 173435 bytes, 0 no buffer
        Received 752 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        752 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/6) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Control Point Interface States:
                Interface number is unassigned
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/2) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Control Point Interface States:
                Interface number is unassigned
Interface Management0/0 "intm00", is up, line protocol is up
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 000f.f775.5412, MTU 1500
        IP address unassigned
        751 packets input, 170487 bytes, 0 no buffer
        Received 753 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/1)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 738 VLAN untagged packets, 156831 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 413 VLAN untagged packets
        Management-only interface. Blocked 0 through-the-device packets
                0 IPv4 packets originated from management network
                0 IPv4 packets destined to management network
                0 IPv6 packets originated from management network
                0 IPv6 packets destined to management network
        Control Point Interface States:
                Interface number is 1
                Interface config status is active
                Interface state is active
Interface GigabitEthernet1/0 "intg10", is down, line protocol is down
  Hardware is VCS7380 rev01, BW 1000 Mbps
```

```
        Auto-Duplex, Auto-Speed
        Media-type configured as RJ45 connector
        MAC address 000b.fcff.b548, MTU 1500
        IP address 17.1.9.115, subnet mask 255.0.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 rate limit drops
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 0 VLAN untagged packets, 0 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 0 VLAN untagged packets
        Control Point Interface States:
                Interface number is 2
                Interface config status is active
                Interface state is not active
...
```

表 7-14 に、**show interface** ***detail*** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 7-9 を参照してください。

表 7-14　show interface detail のフィールド

フィールド	説明
Demux drops	（内部データ インターフェイスのみ）SSM インターフェイスからのパケットをセキュリティ アプライアンスが逆多重化できなかったために、ドロップされたパケットの数。SSM インターフェイスは、バックプレーンを経由してネイティブ インターフェイスと通信し、どの SSM インターフェイスからのパケットもバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	このインターフェイスが作成された順序を示す、デバッグに使用される番号。0 から開始されます。
Interface config status	管理状態。次のいずれかです。 • active：インターフェイスはシャットダウンされていません。 • not active：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Interface state	インターフェイスの実際の状態。ほとんどの場合、この状態は上の config status と一致しています。ハイ アベイラビリティを設定した場合には、セキュリティ アプライアンスは必要に応じてインターフェイスを起動またはシャットダウンするため、一致しない場合があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信された ASR パケット数。
Transmitted X2 packets	このインターフェイスで送信された ASR パケット数。
Dropped X3 packets	このインターフェイスでドロップされた ASR パケット数。パケットがドロップされるのは、パケットを転送しようとしたときにインターフェイスがダウンしている場合です。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタを消去します。
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。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

インターフェイスの IP アドレスとステータスを表示するには、特権 EXEC モードで **show interface ip brief** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] ***ip brief***

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスを表示します。

コマンドのモード

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

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内でのみ指定できます。

表示される出力については、「例」の項を参照してください。

例

次に、**show interface ip brief** コマンドの出力例を示します。

```
hostname# show interface ip brief
    Interface                  IP-Address      OK? Method  Status
Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

表 7-15 に、各フィールドの説明を示します。

表 7-15　show interface ip brief のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名を設定した場合は、その名前。すべてのインターフェイスを表示する場合、AIP SSM 用の内部インターフェイスが ASA 適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報も表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
IP-Address	インターフェイスの IP アドレス。
OK?	このカラムは、現在は使用されていません。常に「Yes」が表示されます。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 • unset：IP アドレスが設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。
Status	管理状態。次のいずれかです。 • up：インターフェイスはシャットダウンされていません。 • administratively down：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Protocol	回線の状態。次のいずれかです。 • up：使用しているケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが誤っているか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show inventory

ネットワーク デバイスにインストールされ、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）を割り当てられているすべてのシスコ製品に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show inventory** コマンドを使用します。シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得されず、表示されません。

show inventory [**slot**]

シンタックスの説明

slot	（オプション）SSM スロット番号を指定します（システムはスロット 0）。

デフォルト

インベントリを表示するスロットを指定しない場合は、次のように処理されます。

- 電源を含めて、すべての SSM のインベントリ情報が表示されます。

コマンドのモード

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)	セマンティックの小さな変更。

使用上のガイドライン

show inventory コマンドは、各シスコ製品のインベントリ情報を UDI 形式で取得し、表示します。UDI は、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）という 3 つの別個のデータ要素を結合したものです。

PID は、製品をご注文いただく際の名称で、従来は「製品名」または「製品番号」と呼ばれていたものです。これは、交換部品を間違いなくご注文いただくために使用する識別子です。

VID は、製品のバージョンです。製品が改良されると、VID が増分します。VID は、製品変更通知（PCN）について規定した業界ガイドラインである Telcordia GR-209-CORE に基づいた、厳格なプロセスに従って増分されます。

SN は、製品に対するベンダー独自の連続番号です。製造される各製品は、製造時に割り当てられる一意のシリアル番号を保持しており、この番号は現場では変更できません。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

UDI では、各製品をエンティティと呼びます。シャーシなどの一部のエンティティは、スロットなどの下位エンティティを保持しています。各エンティティは、シスコ エンティティ別に階層構造で整理された論理的な表示順に従って、1 行に 1 つずつ表示されます。

show inventory コマンドをオプションなしで使用すると、ネットワーク デバイスにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されます。

例

次に、キーワードと引数を指定しない場合の **show inventory** コマンドの出力例を示します。この出力例では、ルータにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されています。

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540            , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20         , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC    , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540            , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20         , VID:V01 , SN:P0000000999
```

表 7-16 に、この出力に表示されるフィールドについて説明します。

表 7-16　show inventory のフィールドの説明

フィールド	説明
Name	シスコ エンティティに割り当てられている物理名（テキスト文字列）。たとえば、デバイスの物理コンポーネント名前付けシンタックスに基づいた、「1」などのコンソール番号または単純なコンポーネント番号（ポート番号やモジュール番号）です。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトの特徴を示す、シスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティの製品 ID。RFC 2737 の entPhysicalModeName MIB 変数に相当します。
VID	エンティティのバージョン ID。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	製品のシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

関連コマンド

コマンド	説明
show diag	ネットワーク デバイスについて、コントローラ、インターフェイス プロセッサ、ポート アダプタの診断情報を表示します。
show tech-support	ルータが問題を報告したときに、ルータに関する一般情報を表示します。

show ip address

インターフェイスの IP アドレスまたは透過モードの管理 IP アドレスを表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスの IP アドレスを表示します。

コマンドのモード

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。

使用上のガイドライン

ハイ アベイラビリティを設定した場合は、現在の IP アドレスとともにプライマリ IP アドレス（表示には「System」と示されます）が表示されます。装置がアクティブになっている場合、システム IP アドレスと現在の IP アドレスは一致します。装置がスタンバイになっている場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

例

次に、**show ip address** コマンドの出力例を示します。

```
hostname# show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

表 7-17 に、各フィールドの説明を示します。

表 7-17　show ip address のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名を設定した場合は、その名前。
Name	**nameif** コマンドで設定したインターフェイス名。
IP address	インターフェイスの IP アドレス。
Subnet mask	IP アドレスとサブネット マスク。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 • unset：IP アドレスが設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

インターフェイスの DHCP リースまたは DHCP サーバに関する詳細情報を表示するには、特権 EXEC モードで **show ip address dhcp** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} ***dhcp*** {***lease*** | ***server***}

シンタックスの説明

interface_name	**nameif** コマンドで設定したインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
server	DHCP サーバに関する情報を表示します。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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、新しいサーバ機能に対応するための ***lease*** キーワードと ***server*** キーワードを含むように変更されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show ip address dhcp lease** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

表 7-18 に、各フィールドの説明を示します。

表 7-18　show ip address dhcp lease のフィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネット マスク。
DHCP Lease server	DHCP サーバのアドレス。
state	DHCP リースの状態。次のいずれかです。 • Initial：初期化状態。セキュリティ アプライアンスがリース取得プロセスを開始します。この状態は、リースが終了したときとリースのネゴシエーションが失敗したときも表示されます。 • Selecting：セキュリティ　アプライアンスは、1　つまたはそれ以上の DHCP サーバから DHCPOFFER メッセージを受信して、いずれかを選択できる状態になるのを待っています。 • Requesting：セキュリティ アプライアンスは、要求の送信先となったサーバからの応答を待っています。 • Purging：セキュリティ アプライアンスは、クライアントが IP アドレスを解放したか、その他の何らかのエラーが発生したために、リースを削除しています。 • Bound：セキュリティ アプライアンスは有効なリースを保持し、正常に動作しています。 • Renewing：セキュリティ アプライアンスは、リースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信して、応答を待ちます。 • Rebinding：セキュリティ　アプライアンスは元のサーバとの間でリースの更新に失敗したため、いずれかのサーバから応答があるか、リースが終了するまで DHCPREQUEST メッセージを送信します。 • Holddown：セキュリティ　アプライアンスは、リースを削除するプロセスを開始しました。 • Releasing：セキュリティ アプライアンスは、IP アドレスが不要になったことを示す解放メッセージをサーバに送信します。
DHCP transaction id	クライアントが選択したランダムな数値。要求メッセージに関連付けるためにクライアントとサーバが使用します。
Lease	DHCP サーバが指定した、インターフェイスがこの IP アドレスを使用できる期間。
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの期間。
Rebind	セキュリティ アプライアンスが DHCP サーバに再バインドしようとするまでの期間。再バインドが発生するのは、セキュリティ アプライアンスが元の DHCP サーバと通信できないまま、リース期間の 87.5% が経過した場合です。この場合、セキュリティ アプライアンスは DHCP 要求をブロードキャストして、使用可能ないずれかの DHCP サーバと通信しようとします。
Temp default-gateway addr	DHCP サーバが提供したデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルトのスタティック ルート。
Next timer fires after	内部タイマーが始動するまでの秒数。

表 7-18　show ip address dhcp lease のフィールド（続き）

フィールド	説明
Retry count	セキュリティ アプライアンスがリースを確立しようとしている場合、このフィールドはセキュリティ アプライアンスが DHCP メッセージの送信を試行した回数を示しています。たとえば、セキュリティ アプライアンスが Selecting 状態になっている場合、この値はセキュリティ アプライアンスが検出メッセージを送信した回数を示しています。セキュリティ アプライアンスが Requesting 状態になっている場合は、セキュリティ アプライアンスが要求メッセージを送信した回数を示しています。
Client-ID	サーバとのすべての通信で使用されるクライアント ID。
Proxy	このインターフェイスが、VPN クライアントのプロキシ DHCP クライアントであるかどうかを示します（True または False）。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 7-19 に、各フィールドの説明を示します。

表 7-19　show ip address dhcp server のフィールド

フィールド	説明
DHCP server	このインターフェイスがリースを取得した DHCP サーバのアドレス。最初のエントリ（「ANY」）はデフォルト サーバで、常に表示されます。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は通常は 1 です。VPN のプロキシとして動作しているインターフェイスに対してサーバがアドレスを提供している場合は、リースが複数になります。
Offers	サーバからのオファーの数。
Requests	サーバに送信した要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した辞退の数。
Releases	サーバに送信したリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバ アドレス。

表 7-19　show ip address dhcp server のフィールド（続き）

フィールド	説明
DNS1	DHCP サーバから取得したセカンダリ DNS サーバ アドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバ アドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバ アドレス。
Subnet	DHCP サーバから取得したサブネット アドレス。
DNS Domain	DHCP サーバから取得したドメイン。

関連コマンド

コマンド	説明
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。
ip address dhcp	DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

インターフェイスに監査ポリシーを適用した場合に、一致したシグニチャの数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

show ip audit count [**global** | **interface** *interface_name*]

シンタックスの説明

global	（デフォルト）すべてのインターフェイスについて、一致した件数を表示します。
interface *interface_name*	（オプション）指定したインターフェイスについて、一致した件数を表示します。

デフォルト

キーワードを指定しない場合は、すべてのインターフェイスについて一致件数が表示されます（***global***）。

コマンドのモード

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。

使用上のガイドライン

監査ポリシーを作成するには **ip audit name** コマンドを使用し、ポリシーを適用するには **ip audit interface** コマンドを使用します。

例

次に、**show ip audit count** コマンドの出力例を示します。

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 A DNS Host Info              0
6051 A DNS Zone Xfer              0
6052 A DNS Zone Xfer High Port    0
6053 A DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

関連コマンド

コマンド	説明
clear ip audit count	監査ポリシーのシグニチャ一致件数を消去します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

show ip verify statistics

Unicast RPF 機能によってドロップされたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。Unicast RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

show ip verify statistics [interface *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）指定したインターフェイスに関する統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスに関する統計情報を表示します。

コマンドのモード

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 ip verify statistics** コマンドの出力例を示します。

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。このコマンドの別の形式である、**show crypto ipsec sa** を使用することもできます。

show ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

シンタックスの説明

detail	（オプション）表示対象に関する詳細なエラー情報を表示します。
entry	（オプション）IPSec SA をピア アドレスでソートして表示します。
identity	（オプション）IPSec SA を ID でソートして、ESP を除いて表示します。これは圧縮された形式です。
map map-name	（オプション）指定した暗号マップの IPSec SA を表示します。
peer peer-addr	（オプション）指定したピア IP アドレスの IPSec SA 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。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、IPSec SA を表示しています。

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、def という暗号マップの IPSec SA を表示しています。

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
```

```
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例では、キーワード ***identity*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、キーワード ***identity*** と ***detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

IPSec SA の要約を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa summary** コマンドを使用します。

show ipsec sa summary

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、次の接続タイプごとに IPSec SA の要約を表示しています。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロードバランシング

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:             Peak IPSec SA's:
IPSec              :     2        Peak Concurrent SA  :    14
IPSec over UDP     :     2        Peak Concurrent L2L :     0
IPSec over NAT-T   :     4        Peak Concurrent RA  :    14
IPSec over TCP     :     6
IPSec VPN LB       :     0
Total              :    14
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA 全体を削除します。または、指定したパラメータに基づいて削除します。
show ipsec sa	IPSec SA のリストを表示します。
show ipsec stats	IPSec に関する一連の統計情報を表示します。

show ipsec stats

一連の IPSec 統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec stats** コマンドを使用します。

show ipsec stats

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、IPSec 統計情報を表示しています。

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA またはカウンタを、指定したパラメータに基づいて消去します。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show ipv6 access-list

IPv6 アクセスリストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセスリストは、どの IPv6 トラフィックがセキュリティ アプライアンスを通過できるかを規定するものです。

show ipv6 access-list [*id* [*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address*]]

シンタックスの説明

any	（オプション）IPv6 プレフィックス ::/0 の短縮形です。
host *source-ipv6-address*	（オプション）特定のホストの IPv6 アドレス。指定した場合は、指定したホストに関するアクセス規則のみが表示されます。
id	（オプション）アクセスリスト名。指定した場合は、指定したアクセスリストのみが表示されます。
source-ipv6-prefix /*prefix-length*	（オプション）IPv6 ネットワーク アドレスとプレフィックス。指定した場合は、指定した IPv6 ネットワークに関するアクセス規則のみが表示されます。

デフォルト

すべての IPv6 アクセスリストを表示します。

コマンドのモード

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

show ipv6 access-list コマンドは、IPv6 固有のものであることを除けば、**show ip access-list** コマンドと同様の出力を提供します。

例

次に、**show ipv6 access-list** コマンドの出力例を示します。inbound、tcptraffic、および outbound という名前の IPv6 アクセスリストが表示されています。

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300
(time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセスリストを作成します。

show ipv6 interface

IPv6 用に設定されているインターフェイスのステータスを表示するには、特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [***brief***] [*if_name* [***prefix***]]

シンタックスの説明

brief	各インターフェイスの IPv6 ステータスとコンフィギュレーションについて、簡単な要約を表示します。
if_name	（オプション）**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。指定したインターフェイスについてのみ、ステータスとコンフィギュレーションが表示されます。
prefix	（オプション）ローカル IPv6 プレフィックス プールから生成されたプレフィックス。

デフォルト

すべての IPv6 インターフェイスを表示します。

コマンドのモード

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

show ipv6 interface コマンドは、IPv6 固有のものであることを除けば、**show interface** コマンドと同様の出力を提供します。インターフェイス ハードウェアが使用可能な場合、そのインターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されます。

例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、***brief*** キーワードを指定して入力した **show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 neighbor

IPv6 近隣探索キャッシュ情報を表示するには、特権 EXEC モードで **show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbor [*if_name* | *address*]

シンタックスの説明

address	（オプション）指定した IPv6 アドレスの近隣探索キャッシュ情報だけを表示します。
if_name	（オプション）指定したインターフェイス名（**nameif** コマンドによって設定）のキャッシュ情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

次に、**show ipv6 neighbor** コマンドによって提供される情報を示します。

- **IPv6 Address**：ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age**：アドレスが到達可能と確認された時点からの経過時間（分単位）。ハイフン（-）は、スタティック エントリであることを示します。
- **Link-layer Addr**：MAC アドレス。アドレスが不明な場合は、ハイフン（-）が表示されます。
- **State**：近隣キャッシュ エントリの状態。

（注） 到達可能性の検出は、IPv6 近隣探索キャッシュのスタティック エントリには適用されません。したがって、**INCMP**（不完全）状態と **REACH**（到達可能）状態の説明は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 近隣探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- **INCMP**：（不完全）このエントリのアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージをまだ受信していません。
- **REACH**：（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。**REACH** 状態になっている間は、パケットが送信されるときにデバイスは特に操作を実行しません。

- **STALE**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。**STALE** 状態になっている間は、パケットが送信されるまで、デバイスは操作を一切実行しません。
- **DELAY**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。パケットは、直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。**DELAY** 状態に入ってから DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認が受信されない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE**：到達可能性確認が受信されるまで、RetransTime ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認を要求し続けます。
- **????**：不明な状態。

次に、IPv6 近隣探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- **INCMP**：（不完全）このエントリのインターフェイスはダウンしています。
- **REACH**：（到達可能）このエントリのインターフェイスは動作しています。

- **Interface**

  アドレスに到達可能であったインターフェイス。

例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。
ipv6 neighbor	IPv6 近隣探索キャッシュ内にスタティック エントリを設定します。

show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 route** コマンドを使用します。

show ipv6 route

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。

コマンドのモード

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

show ipv6 route コマンドは、情報が IPv6 固有のものであることを除けば、**show route** コマンドと同様の出力を提供します。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- **Codes**：ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - **C**：接続済み
  - **L**：ローカル
  - **S**：スタティック
  - **R**：RIP 生成
  - **B**：BGP 生成
  - **I1**：ISIS L1：統合 IS-IS Level 1 生成
  - **I2**：ISIS L2：統合 IS-IS Level 2 生成
  - **IA**：ISIS エリア間：統合 IS-IS エリア間生成
- **fe80::/10**：リモート ネットワークの IPv6 プレフィックスを示します。
- **[0/0]**：カッコ内の最初の数値は、情報ソースの管理ディスタンスです。2 番目の数値はルートのメトリックです。
- **via ::**：リモート ネットワークに到達するための次のルータのアドレスを示します。
- **inside**：示されているネットワークへの次のルータに到達できるインターフェイスを示します。

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 routers

オンリンク ルータから受信した IPv6 ルータ アドバタイズメント情報を表示するには、特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

show ipv6 routers [*if_name*]

シンタックスの説明

if_name	（オプション）情報を表示する対象となる、**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されます。

例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

show ipv6 traffic

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。

コマンドのモード

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

トラフィック カウンタを消去するには、**clear ipv6 traffic** コマンドを使用します。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

関連コマンド

コマンド	説明
clear ipv6 traffic	IPv6 トラフィック カウンタを消去します。

show isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp sa** コマンドを使用します。

show isakmp sa [**detail**]

シンタックスの説明

detail	SA データベースに関する詳細な出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合：

表 7-20

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合：

表 7-21

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

グローバル コンフィギュレーション モードで入力した次の例では、SA データベースに関する詳細な情報を表示しています。

```
hostname(config)# show isakmp sa detail
hostname(config)# sho isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

実行時の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp stats** コマンドを使用します。

show isakmp stats

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。

コマンドのモード

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	•	•	•	—	—
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

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels

- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show local-host

ローカル ホストのネットワーク状態を表示するには、特権 EXEC モードで **show local-host** コマンドを使用します。

show local-host [*ip_address*] [**detail**] [**all**]

シンタックスの説明

all	（オプション）ローカル ホスト状態のホストが作成した接続のリストを含めることを指定します。セキュリティ アプライアンスに向かう接続、およびセキュリティ アプライアンスからの接続が含まれます。
detail	（オプション）ローカル ホストの詳細なネットワーク状態情報を表示します。
ip_address	（オプション）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show local-host コマンドを使用すると、ローカル ホストのネットワーク状態を表示できます。ローカル ホストは、トラフィックをセキュリティ アプライアンスに転送するか、セキュリティ アプライアンスを通じて転送するすべてのホストに対して作成されます。

このコマンドを使用すると、ローカル ホストの変換スロットと接続スロットを表示したり、これらのホスト上のすべてのトラフィックを停止したりできます。また、標準の変換状態および接続状態が適用されない場合、**nat 0** ***access-list*** コマンドで設定されたホストの情報を提供します。

show local-host detail コマンドは、アクティブな xlate とネットワーク接続に関する詳細情報を表示します。

1 つのホストの情報だけを表示するには、*ip_address* 引数を使用します。

ローカル ホストが作成した接続を一覧表示するには、**all** キーワードを使用します。セキュリティ アプライアンスに向かう接続、およびセキュリティ アプライアンスからの接続が含まれます。**all** キーワードを使用しない場合、セキュリティ アプライアンスに向かうローカル ホスト接続、およびセキュリティ アプライアンスからのローカル ホスト接続は表示されません。

このコマンドは、接続制限値を表示します。接続制限を設定していない場合、この値には 0 が表示され、制限は適用されません。

TCP 代行受信を設定した場合は、SYN 攻撃が発生すると、代行受信された接続の数が **show local-host** コマンドの出力の使用状況カウントに含まれます。このフィールドには、通常は完全にオープンな接続のみが表示されます。

show local-host コマンドの出力で TCP embryonic count to host counter が使用されるのは、スタティック接続を使用するホストに対して最大初期接続数の制限（TCP 代行受信の水準点）を設定した場合です。このカウンタは、他のホストからこのホストに向かう初期接続の合計数を示しています。この合計数が設定済みの制限値を超えると、このホストに向かう新しい接続に TCP 代行受信が適用されます。

例

次の例は、ローカル ホストのネットワーク状態を表示する方法を示しています。

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied
```

```
hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1
active, 1 maximum active, 0 denied
```

関連コマンド

コマンド	説明
clear local-host	***show local-host*** コマンドで表示された、ローカル ホストからのネットワーク接続を解放します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show logging

バッファに保持されているログ、またはその他のロギング設定を表示するには、**show logging** コマンドを使用します。

show logging [**message** [*syslog_id* | **all**] | **asdm** | ***queue*** | ***setting***]

シンタックスの説明

message	（オプション）デフォルト以外のレベルのメッセージを表示します。メッセージ レベルを設定するには、**logging message** コマンドを参照してください。
syslog_id	（オプション）表示するメッセージ番号を指定します。
all	（オプション）イネーブルまたはディセーブルのどちらになっているかを含めて、すべての syslog メッセージ ID を表示します。
setting	（オプション）ロギング設定を表示します。ロギング バッファは表示しません。
asdm	（オプション）ASDM ロギング バッファの内容を表示します。
queue	（オプション）syslog メッセージ キューを表示します。

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。

コマンドのモード

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。

使用上のガイドライン

logging buffered コマンドを使用している場合は、キーワードを指定せずに **show logging** コマンドを実行すると、現在のメッセージ バッファと設定が表示されます。

show logging queue コマンドを使用すると、次の情報を表示できます。

- キュー内のメッセージ数
- キューに記録されたメッセージの最大数
- 処理に利用できるブロック メモリがなかったために廃棄されたメッセージ数

例

次に、**show logging** コマンドの出力例を示します。

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

次に、**show logging message all** コマンドの出力例を示します。

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

関連コマンド

コマンド	説明
logging asdm	ASDM へのロギングをイネーブルにします。
logging buffered	バッファへのロギングをイネーブルにします。
logging message	メッセージ レベルを設定します。または、メッセージをディセーブルにします。
logging queue	ロギング キューを設定します。

show logging rate-limit

禁止されたメッセージを元の設定で表示するには、**show logging rate-limit** コマンドを使用します。

show logging rate-limit

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。

コマンドのモード

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	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

情報がクリアされると、ホストが接続を再び確立するまで、何も表示されません。

例

次の例は、禁止されたメッセージを表示する方法を示しています。

```
hostname(config)# show logging rate-limit
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

show mac-address-table [*interface_name* | **count** | **static]**

シンタックスの説明

count	（オプション）ダイナミック エントリとスタティック エントリの総数を表示します。
interface_name	（オプション）MAC アドレス テーブル エントリを表示するインターフェイス名を指定します。
static	（オプション）スタティック エントリのみ表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスの MAC アドレス エントリが表示されます。

コマンドのモード

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 mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table
interface          mac address       type      Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、inside というインターフェイスに関する **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show management-access

管理アクセス用に設定されている内部インターフェイスの名前を表示するには、特権 EXEC モードで show management-access コマンドを使用します。

show management-access

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。

コマンドのモード

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。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は、**nameif** コマンドで定義します。**show interface** コマンドの出力では、二重引用符（"）で囲まれて表示されます）。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show memory

物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示するには、特権 EXEC モードで **show memory** コマンドを使用します。

show memory [**detail**]

シンタックスの説明

detail	（オプション）空きシステム メモリと割り当て済みシステム メモリの詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show memory コマンドを使用すると、オペレーティング システムで使用できる最大物理メモリと現在の空きメモリの要約を表示することができます。メモリは、必要に応じて割り当てられます。

show memory detail コマンドの出力を **show memory binsize** コマンドで利用すると、メモリ リークをデバッグすることができます。

また、SNMP を使用して **show memory** コマンドからの情報を表示することもできます。

例

次の例は、使用できる最大物理メモリと現在の空きメモリの要約を表示する方法を示しています。

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

次の例は、メモリに関する詳細な出力を示しています。

```
hostname# show memory detail
Free memory: 15958088 bytes (24%)
Used memory:
Allocated memory in use: 29680332 bytes (44%)
Reserved memory: 21470444 bytes (32%)
---------------------------- ----------------
Total memory: 67108864 bytes (100%)

Least free memory: 4551716 bytes ( 7%)
Most used memory: 62557148 bytes (93%)

----- fragmented memory statistics -----
```

```
fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
16 8 128
24 4 96
32 2 64
40 5 200
64 3 192
88 1 88
168 1 168
224 1 224
256 1 256
296 2 592
392 1 392
400 1 400
1816 1 1816*
4435968 1 4435968**
11517504 1 11517504

* - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
40 50 2000
48 144 6912
56 24957 1397592
64 101 6464
72 99 7128
80 1032 82560
88 18 1584
96 64 6144
104 57 5928
112 6 672
120 112 13440
128 15 1920
136 87 11832
144 22 3168
152 31 4712
160 90 14400
168 65 10920
176 74 13024
184 11 2024
192 8 1536
200 1 200
< 以下省略 >
```

関連コマンド

コマンド	説明
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory binsize

特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示するには、特権 EXEC モードで ***show memory binsize*** コマンドを使用します。

show memory binsize *size*

シンタックスの説明

size	（オプション）特定のバイナリ サイズのチャンク（メモリ ブロック）を表示します。バイナリ サイズは、***show memory detail*** コマンドの出力の「fragment size」カラムに示されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

このコマンドに使用上のガイドラインはありません。

例

次の例では、バイナリ サイズ 500 が割り当てられているチャンクに関する要約情報を表示しています。

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

関連コマンド

コマンド	説明
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレスの範囲を表示します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。

show memory profile

セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示するには、特権 EXEC モードで ***show memory profile*** コマンドを使用します。

show memory profile [peak] [detail | collated | status]

シンタックスの説明

collated	（オプション）表示されるメモリ情報を整形します。
detail	（オプション）メモリの詳細情報を表示します。
peak	（オプション）「使用中の」バッファではなく、ピーク キャプチャ バッファを表示します。
status	（オプション）メモリ プロファイリングの現在の状態とピーク キャプチャ バッファを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show memory profile コマンドは、メモリ使用状況レベルとメモリ リークをトラブルシューティングするために使用します。プロファイル バッファの内容は、プロファイリングを停止した場合でもまだ参照できます。プロファイリングを開始すると、バッファは自動的に消去されます。

（注）　メモリのプロファイリングをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスが一時的に低下することがあります。

例

次のように表示されます。

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

次に示す **show memory profile detail** コマンドの出力は、6 つのデータ カラムと 1 つのヘッダー カラムに区分され、左揃えで表示されています。ヘッダー カラムには、先頭のデータ カラムのメモリ バケットのアドレスが表示されます（16 進値）。データ自体は、バケット アドレスにあるテキストまたはコードが保持しているバイト数です。データ カラム内のピリオド（.）は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケット アドレスを表しています。たとえば、最初の行の先頭のデータ カラムのアドレス バケットは 0x001069e0 です。最初の行の 2 番目のデータ カラムのアドレス バケットは 0x001069e4 で、以降も同様に増分していきます。通常は、ヘッダー カラムにあるアドレスが次のバケット アドレスです。これは、前の行の最後のデータ カラムのアドレスに増分値を加算したものです。使用状況を含んでいない行は、一切表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダー カラムに 3 個のピリオド（...）で示されます。

```
hostname# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
< 省略 >
```

次に、整形された出力の例を示します。

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
< 省略 >
```

次の例では、ピーク キャプチャ バッファを表示しています。

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次の例では、ピーク キャプチャ バッファ、および当該バケット アドレスにあるテキストまたはコードが保持しているバイト数を表示しています。

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

次の例では、メモリ プロファイリングの現在の状態とピーク キャプチャ バッファを表示しています。

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能が保持しているメモリ バッファを消去します。

show memory-caller address

セキュリティ アプライアンス上に設定されているアドレス範囲を表示するには、特権 EXEC モードで ***show memory-caller address*** コマンドを使用します。

show memory-caller address

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。

コマンドのモード

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

show memory-caller address コマンドを使用してアドレス範囲を表示するには、***memory caller-address*** コマンドを使用して、アドレス範囲をあらかじめ設定しておく必要があります。

例

次の例は、***memory caller-address*** コマンドで設定したアドレス範囲、および ***show memory-caller address*** コマンドによる表示結果を示しています。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

アドレス範囲を設定する前に ***show memory-caller addresss*** コマンドを入力した場合、アドレスは表示されません。

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

関連コマンド

コマンド	説明
memory caller-address	呼び出し側 PC のメモリ ブロックを設定します。

show mfib

転送する側のエントリおよびインターフェイスに関する MFIB を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib** コマンドを使用します。

show mfib [*group* [*source*]] [***verbose***]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。
verbose	（オプション）エントリの詳細な情報を表示します。

デフォルト

オプションの引数を指定しない場合は、すべてのグループの情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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 mfib** コマンドの出力例を示します。

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib verbose	転送する側のエントリおよびインターフェイスに関する詳細な情報を表示します。

show mfib active

アクティブなマルチキャスト送信元を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib active** コマンドを使用します。

show mfib [*group*] **active** [*kbps*]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
kbps	（オプション）この値以上のレートで送信されているマルチキャスト ストリームのみを表示します。

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

kbps のデフォルト値は 4 です。*group* を指定しない場合は、すべてのグループが表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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

show mfib active コマンドの出力では、PPS のレートに正または負の数値が表示されます。セキュリティ アプライアンスが負の数値を表示するのは、RPF パケットが失敗した場合か、ルータが発信インターフェイス（OIF）リストを使用して RPF パケットを監視している場合です。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

例

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

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

関連コマンド

コマンド	説明
show mroute active	アクティブなマルチキャスト ストリームを表示します。

show mfib count

MFIB ルートおよびパケットの数に関するデータを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib count** コマンドを使用します。

show mfib [*group* [*source*]] **count**

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、パケットのドロップに関する統計情報を表示します。

例

次に、**show mfib count** コマンドの出力例を示します。

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

関連コマンド

コマンド	説明
clear mfib counters	MFIB ルータ パケットのウンタを消去します。
show mroute count	マルチキャスト ルートのカウンタを表示します。

show mfib interface

MFIB プロセスに関係しているインターフェイスのパケット統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib interface** コマンドを使用します。

show mfib interface [*interface*]

シンタックスの説明

interface	（オプション）インターフェイス名を指定します。指定したインターフェイスに関する情報のみを表示します。

デフォルト

すべての MFIB インターフェイスに関する情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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 mfib interface** コマンドの出力例を示します。

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib reserved

予約済みグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib reserved** コマンドを使用します。

show mfib reserved [***count*** | ***verbose*** | ***active*** [*kpbs*]]

シンタックスの説明

count	（オプション）パケットおよびルートの数に関するデータを表示します。
verbose	（オプション）詳細な情報を表示します。
active	（オプション）アクティブなマルチキャスト送信元を表示します。
kpbs	（オプション）この値以上のレートで送信を実行している、アクティブなマルチキャスト送信元のみを表示します。

デフォルト

kbps のデフォルト値は 4 です。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、224.0.0.0 ～ 224.0.0.225 の範囲にある MFIB エントリを表示します。

例

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

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

関連コマンド

コマンド	説明
show mfib active	アクティブなマルチキャスト ストリームを表示します。

show mfib status

MFIB の全般的なコンフィギュレーションと動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib status** コマンドを使用します。

show mfib status

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。

コマンドのモード

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
ユーザ EXEC または特権 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 mfib status** コマンドの出力例を示します。

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib summary

MFIB のエントリおよびインターフェイスの数に関する要約情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib summary** コマンドを使用します。

show mfib summary

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。

コマンドのモード

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
ユーザ EXEC または特権 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 mfib summary** コマンドの出力例を示します。

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

関連コマンド

コマンド	説明
show mroute summary	マルチキャスト ルーティング テーブルの要約情報を表示します。

show mfib verbose

転送する側のエントリおよびインターフェイスに関する詳細情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib verbose** コマンドを使用します。

show mfib verbose

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。

コマンドのモード

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
ユーザ EXEC または特権 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 mfib verbose** コマンドの出力例を示します。

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show mfib summary	MFIB のエントリおよびインターフェイスの数に関する要約情報を表示します。

show mgcp

MGCP のコンフィギュレーションとセッション情報を表示するには、特権 EXEC モードで **show mgcp** コマンドを使用します。

show mgcp {*commands* | *sessions*} [*detail*]

シンタックスの説明

コマンド	コマンド キューに含まれている MGCP コマンドの数を表示します。
sessions	既存の MGCP セッションの数を表示します。
detail	（オプション）各コマンド（またはセッション）に関する追加情報を出力に含めます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド（またはセッション）に関する追加情報を出力に含めます。

例

次に、**show mgcp** コマンド オプションの例を示します。

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058

hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug mgcp	MGCP デバッグ情報をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。

show mode

実行中のソフトウェア イメージおよびフラッシュ メモリに保持されている任意のイメージについて、セキュリティ コンテキスト モードを表示するには、特権 EXEC モードで **show mode** コマンドを使用します。

show mode

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。

コマンドのモード

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	このコマンドが導入されました。

例

次に、**show mode** コマンドの出力例を示します。ここでは、現在のモード、および実行されていないイメージ「image.bin」のモードを表示しています。

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

モードは、マルチまたはシングルのいずれかです。

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
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 module

ASA 5500 シリーズ適応型セキュリティ アプライアンス上の SSM に関する情報をシステム情報とともに表示するには、ユーザ EXEC モードで **show module** コマンドを使用します。

show module [*slot* [***details***] | **all** | **1** ***recover***]]

シンタックスの説明

all	（デフォルト）スロット 1 の SSM およびスロット 0 のシステムに関する情報を表示します。
details	（オプション）インテリジェント SSM（AIP SSM など）のリモート管理コンフィギュレーションを含めて、詳細な情報を表示します。
1 recover	（オプション）インテリジェント SSM について、**hw-module module recover** コマンドの設定を表示します。
slot	（オプション）スロット番号（0 または 1）を指定します。

デフォルト

両方のスロットの情報を表示します。

コマンドのモード

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[1]	システム
ユーザ EXEC	•	•	•	•	•

1. **show module recover** コマンドを使用できるのは、システム実行スペース内のみです。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SSM に関する情報をシステムおよび組み込みインターフェイスの情報とともに表示します。

表示される出力については、「例」の項を参照してください。

例

次に、**show module** コマンドの出力例を示します。スロット 0 はシステムで、スロット 1 は SSM です。

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            XXXXXXXXXXX
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         XXXXXXXXXXX

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c619 to 000b.fcf8.c61d  1.0          1.0(6)5      7.0(0)77
  1 000b.fcf8.019f to 000b.fcf8.019f  1.0          1.0(6)5      5.0(0.15)S91(0.15)

Mod Status
--- ------------------
  0 Up Sys
  1 Up
```

表 7-22 に、各フィールドの説明を示します。

表 7-22　show module のフィールド

フィールド	説明
Mod	スロット番号（0 または 1）。
Card Type	スロット 0 にあるシステムの場合、タイプはプラットフォーム モデルです。スロット 1 にある SSM の場合は、SSM のタイプです。
Model	このスロットのモデル。
Serial No.	シリアル番号。
MAC Address Range	この SSM 上のインターフェイス、システム、または組み込みインターフェイスの MAC アドレス範囲。
Hw Version	ハードウェアのバージョン。
Fw Version	ファームウェアのバージョン。
Sw Version	ソフトウェアのバージョン。
Status	スロット 1 にあるシステムの場合、ステータスは Up Sys です。スロット 1 にある SSM のステータスは、次のいずれかです。 • Initializing：SSM は検出中で、制御接続はシステムによって初期化中です。 • Up：SSM は、システムによる初期化が完了しています。 • Unresponsive：システムがこの SSM と通信しているときに、エラーが発生しました。 • Reloading：インテリジェント SSM である場合に、SSM がリロード中です。 • Shutting Down：SSM はシャットダウン中です。 • Down：SSM はシャットダウンしました。 • Recover：インテリジェント SSM である場合に、SSM がリカバリ イメージをダウンロードしようとしています。

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

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

表 7-23 に、各フィールドの説明を示します。**show module** コマンドでも表示されるフィールドについては、表 7-22 を参照してください。

表 7-23　show module details のフィールド

フィールド	説明
Mgmt IP addr	インテリジェント SSM について、SSM 管理インターフェイスの IP アドレスを表示します。
Mgmt web ports	インテリジェント SSM について、管理インターフェイス用に設定されているポートを表示します。
Mgmt TLS enabled	インテリジェント SSM について、SSM の管理インターフェイスへの接続でトランスポート レイヤ セキュリティがイネーブルになっているかどうかを表示します（true または false）。

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

```
hostname> show module 1 recover
Module 1 recover parameters…
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。

show mrib client

MRIB クライアント接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib client** コマンドを使用します。

show mrib client [***filter***] [***name*** *client_name*]

シンタックスの説明

filter	（オプション）クライアント フィルタを表示します。各クライアントの所有する MRIB フラグ、および各クライアントと関連のあるフラグに関する情報を表示するために使用します。
name *client_name*	（オプション）MRIB のクライアントとして機能する、PIM や IGMP などのマルチキャスト ルーティング プロトコルの名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

filter オプションは、さまざまな MRIB クライアントが登録した、ルートおよびインターフェイス レベルのフラグの変化を表示するために使用します。このコマンド オプションを指定すると、どのフラグが MRIB クライアントによって所有されているかも表示されます。

例

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

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブル のエントリを表示します。

show mrib route

MRIB テーブルに含まれているエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib route** コマンドを使用します。

show mrib route [[*source* | *****] [*group*[/*prefix-length*]]]

シンタックスの説明

*	（オプション）共有ツリー エントリを表示します。
/prefix-length	（オプション）MRIB ルートのプレフィックスの長さ。アドレスの上位連続ビットの数を示す 10 進値がプレフィックスになります（アドレスのネットワーク部分）。10 進値の前にスラッシュを付ける必要があります。
group	（オプション）グループの IP アドレスまたは名前。
source	（オプション）ルート送信元の IP アドレスまたは名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

MFIB テーブルは、MRIB からアップデートされるエントリとフラグのサブセットを管理します。フラグは、マルチキャスト パケットに関する一連の転送規則に従って、転送とシグナリングの動作を決定するものです。

インターフェイスとフラグのリストに加えて、ルート エントリごとにさまざまなカウンタも表示されます。バイト数は、転送された総バイト数です。パケット数は、このエントリで受信したパケットの数です。**show mfib count** コマンドは、ルートとは無関係にグローバルなカウンタを表示します。

例

次に、**show mrib route** コマンドの出力例を示します。

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

関連コマンド

コマンド	説明
show mfib count	MFIB テーブルのルートおよびパケットの数に関するデータを表示します。
show mrib route summary	MRIB テーブル エントリの要約を表示します。

show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、特権 EXEC モードで **show mroute** コマンドを使用します。

show mroute [*group* [*source*] | ***reserved***] [***active*** [*rate*] | ***count*** | ***pruned*** | ***summary***]

シンタックスの説明

active rate	（オプション）アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定した *rate* 以上で送信を実行している送信元です。*rate* を指定しない場合、アクティブな送信元は 4 Kbps 以上のレートで送信を実行している送信元です。
count	（オプション）グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。
group	（オプション）DNS（ドメイン ネーム システム）ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。
pruned	（オプション）プルーニングされたルートを表示します。
reserved	（オプション）予約済みグループを表示します。
source	（オプション）送信元のホスト名または IP アドレス。
summary	（オプション）マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。

デフォルト

rate 引数を指定しない場合、デフォルトでは 4 Kbps になります。

コマンドのモード

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

show mroute コマンドは、マルチキャスト ルーティング テーブルの内容を表示します。セキュリティ アプライアンスは、PIM プロトコル メッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) エントリと (*,G) エントリを作成し、マルチキャスト ルーティング テーブルにデータを入力します。アスタリスク（*）はすべての送信元アドレス、「S」は単一の送信元アドレス、「G」は宛先マルチキャスト グループ アドレスを意味します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で（RPF を経由して）見つかった該当する宛先グループへの最適パスを使用します。

実行コンフィギュレーションに含まれている **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**show mroute** コマンドの出力例を示します。

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute の出力には、次のフィールドが含まれています。

- **Flags**：エントリに関する情報を提供します。
  - **D（Dense）**：エントリは稠密モードで動作しています。
  - **S（Sparse）**：エントリは希薄モードで動作しています。
  - **B :（Bidir Group）**：マルチキャスト グループが双方向モードで動作していることを示します。
  - **s（SSM Group）**：マルチキャスト グループが SSM の IP アドレス範囲に入っていることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
  - **C（Connected）**：マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
  - **L（Local）**：セキュリティ アプライアンス自体が、マルチキャスト グループのメンバーです。グループは、（設定済みのグループに対する）**igmp join-group** コマンドによってローカルに加入されています。
  - **I（Received Source Specific Host Report）**：(S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。
  - **P（Pruned）**：ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。
  - **R（RP-bit set）**：(S,G) エントリが RP をポイントしていることを示します。
  - **F（Register flag）**：ソフトウェアがマルチキャスト送信元に登録されていることを示します。
  - **T（SPT-bit set）**：パケットが最短パス送信元ツリーで受信されていることを示します。
  - **J（Join SPT）**：(*,G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 Kbps です）。J - Join 最短パス ツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join メッセージがトリガーされます。これにより、セキュリティ アプライアンスは送信元ツリーに加入します。

(S,G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、セキュリティ アプライアンスは送信元ツリー上のトラフィック速度をモニタします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとします。

（注）　セキュリティ アプライアンスは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*,G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*,G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、セキュリティ アプライアンスは最短パス送信元ツリーにただちに切り替えます。

- **Timers:Uptime/Expires** : Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
- **Interface state**：着信インターフェイスまたは発信インターフェイスの状態を示します。
  - **Interface**：着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。
  - **State** : アクセスリストまたは Time to Live（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。
- **(*, 239.1.1.40)** と **(* , 239.2.2.1)** : IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元を意味します。
- **RP**：RP のアドレス。希薄モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 224.0.0.0 です。
- **Incoming interface**：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- **RPF nbr**：送信元に対するアップストリーム ルータの IP アドレス。
- **Outgoing interface list**：パケット転送時に使用されるインターフェイス。

関連コマンド

コマンド	説明
clear configure mroute	**mroute** コマンドを実行コンフィギュレーションから削除します。
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	設定されているマルチキャスト ルートを表示します。

show nameif

nameif コマンドを使用して設定されているインターフェイス名を表示するには、特権 EXEC モードで show nameif コマンドを使用します。

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

シンタックスの説明

mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス名を表示します。

コマンドのモード

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。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内でのみ指定できます。このコマンドの出力では、Interface カラムにはマッピング名のみが示されます。

例

次に、**show nameif** コマンドの出力例を示します。

```
hostname# show nameif
Interface                Name                 Security
GigabitEthernet0/0       outside              0
GigabitEthernet0/1       inside               100
GigabitEthernet0/2       test2                50
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ntp associations

NTP アソシエーションの情報を表示するには、ユーザ EXEC モードで **show ntp associations** コマンドを使用します。

show ntp associations [**detail**]

シンタックスの説明

detail	（オプション）各アソシエーションの詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

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

```
hostname> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

表 7-24 に、各フィールドの説明を示します。

表 7-24　show ntp associations のフィールド

フィールド	説明
（表示行の行頭の文字）	表示行の行頭には、次の文字が 1 つまたはそれ以上表示されます。 • *：このピアに同期しています。 • #：このピアに対してほぼ同期しています。 • +：ピアは同期可能な対象として選択されています。 • -：ピアが選択候補です。 • ~：ピアがスタティックに設定されていますが、同期していません。
address	NTP ピアのアドレス。
ref clock	ピアのリファレンス クロックのアドレス。
st	ピアの層。

表 7-24　show ntp associations のフィールド（続き）

フィールド	説明
when	ピアから最終 NTP パケットが受信されてからの時間。
poll	ポーリング間隔（秒）。
reach	ピアの到達可能性（8 進のビット文字列）。
delay	ピアまでのラウンド トリップ遅延（ミリ秒）。
offset	ローカル クロックに対するピア クロックの相対時間（ミリ秒）。
disp	分散値。

次に、***show ntp associations detail*** コマンドの出力例を示します。

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

表 7-25 に、各フィールドの説明を示します。

表 7-25　show ntp associations detail のフィールド

フィールド	説明
IP-address configured	サーバ（ピア）の IP アドレス。
（ステータス）	• our_master：セキュリティ アプライアンスがこのピアに対して同期しています。 • selected：ピアは同期可能な対象として選択されています。 • candidate：ピアが選択候補です。
（健全性）	• sane：ピアが基本健全性チェックをパスしました。 • insane：ピアが基本健全性チェックで失敗しました。
（有効性）	• valid：ピア時間は有効であるとみなされています。 • invalid：ピア時間は無効であるとみなされています。 • leap_add：ピアが、うるう秒が加算されることをシグナリングしています。 • leap-sub：ピアが、うるう秒が減算されることをシグナリングしています。
stratum	ピアの層。
（リファレンス ピア）	unsynced：ピアは、他のどのマシンにも同期されていません。 ref ID：ピアの同期対象となるマシンのアドレス。
time	ピアがマスターから受信した最終タイムスタンプ。
our mode client	ピアに対する相対的なモード。常に「クライアント」です。

表 7-25　show ntp associations detail のフィールド（続き）

フィールド	説明
peer mode server	ピアの相対的なモード。常に「サーバ」です。
our poll intvl	ピアに対するポーリング間隔。
peer poll intvl	ピアからのポーリング間隔。
root delay	ルートへのパスに沿った遅延（最上位層 1 のタイム ソース）。
root disp	ルートへのパスの分散。
reach	ピアの到達可能性（8 進のビット文字列）。
sync dist	ピアの同期間隔。
delay	ピアまでのラウンド トリップ遅延。
offset	クロックに対するピア クロックのオフセット。
dispersion	ピア クロックの分散。
precision	ピア クロックの精度（ヘルツ）。
version	ピアが使用中の NTP バージョン番号。
org time	開始時のタイムスタンプ。
rcv time	受信時のタイムスタンプ。
xmt time	送信時のタイムスタンプ。
filtdelay	各サンプルのラウンドトリップ遅延（ミリ秒）。
filtoffset	各サンプルのクロック オフセット（ミリ秒）。
filterror	各サンプルの誤差の概算値。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show ntp status

各 NTP アソシエーションのステータスを表示するには、ユーザ EXEC モードで **show ntp status** コマンドを使用します。

show ntp status

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。

コマンドのモード

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
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

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

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

表 7-26 に、各フィールドの説明を示します。

表 7-26　show ntp status のフィールド

フィールド	説明
Clock	• synchronized : セキュリティ アプライアンスが NTP サーバに対して同期しています。 • unsynchronized : セキュリティ アプライアンスが NTP サーバに対して同期していません。
stratum	このシステムの NTP 層。
reference	セキュリティ アプライアンスの同期対象になる NTP サーバのアドレス。
nominal freq	システム ハードウェア クロックの公称周波数。
actual freq	システム ハードウェア クロックの測定周波数。
precision	このシステムのクロックの精度（ヘルツ）。
reference time	参照時のタイムスタンプ。

表 7-26　show ntp status のフィールド（続き）

フィールド	説明
clock offset	同期されたピアに対するシステム クロックのオフセット。
root delay	ルート クロックまでのパスに沿った合計遅延。
root dispersion	ルート パスの分散。
peer dispersion	同期されたピアの分散。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。

show ospf

OSPF ルーティング プロセスに関する一般情報を表示するには、特権 EXEC モードで **show ospf** コマンドを使用します。

show ospf [*pid* [*area_id*]]

シンタックスの説明

area_id	（オプション）OSPF アドレス範囲に関連付けられているエリアの ID。
pid	（オプション）OSPF プロセスの ID。

デフォルト

pid を指定しない場合は、すべての OSPF プロセスが一覧表示されます。

コマンドのモード

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。

使用上のガイドライン

pid を指定すると、指定したルーティング プロセスの情報だけが表示されます。

例

次に、**show ospf** コマンドの出力例を示します。この例は、特定の OSPF ルーティング プロセスに関する一般情報を表示する方法を示しています。

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

次の **show ospf** コマンドの出力例は、すべての OSPF ルーティング プロセスに関する一般情報を表示する方法を示しています。

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf border-routers

ABR および ASBR に対する内部 OSPF ルーティング テーブル エントリを表示するには、特権 EXEC モードで **show ospf border-routers** コマンドを使用します。

show ospf border-routers

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。

コマンドのモード

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 ospf border-routers** コマンドの出力例を示します。

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf database

セキュリティ アプライアンス上の OSPF トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show ospf database** コマンドを使用します。

show ospf [*pid* [*area_id*]] **database** [***router*** | ***network*** | ***summary*** | ***asbr-summary*** | ***external*** | ***nssa-external***] [*lsid*] [***internal***] [***self-originat***e | ***adv-router*** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

シンタックスの説明

addr	（オプション）ルータのアドレス。
adv-router	（オプション）アドバタイズされたルータ。
area_id	（オプション）OSPF アドレス範囲に関連付けられているエリアの ID。
asbr-summary	（オプション）ASBR リストの要約を表示します。
database	データベース情報を表示します。
database-summary	（オプション）データベース全体の要約リストを表示します。
external	（オプション）指定した自律システムの外部のルートを表示します。
internal	（オプション）指定した自律システム内部のルート。
lsid	（オプション）LSA ID。
network	（オプション）ネットワークに関する OSPF データベース情報を表示します。
nssa-external	（オプション）外部準スタブ エリアのリストを表示します。
pid	（オプション）OSPF プロセスの ID。
router	（オプション）ルータを表示します。
self-originate	（オプション）指定した自律システムに関する情報を表示します。
summary	（オプション）リストの要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

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

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

次に、**show ospf database asbr-summary** コマンドの出力例を示します。

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

次に、**show ospf database router** コマンドの出力例を示します。

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

次に、**show ospf database network** コマンドの出力例を示します。

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

次に、**show ospf database summary** コマンドの出力例を示します。

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次に、**show ospf database external** コマンドの出力例を示します。

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf flood-list

インターフェイスを介してフラッドされるのを待機している OSPF LSA のリストを表示するには、特権 EXEC モードで **show ospf flood-list** コマンドを使用します。

show ospf flood-list *interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

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

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf interface

OSPF 関連のインターフェイス情報を表示するには、特権 EXEC モードで **show ospf interface** コマンドを使用します。

show ospf interface [*interface_name*]

シンタックスの説明

interface_name	（オプション）OSPF 関連の情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

interface_name 引数を指定せずに使用すると、すべてのインターフェイスの OSPF 情報が表示されます。

例

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

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開きます。

show ospf neighbor

インターフェイスごとの OSPF ネイバー情報を表示するには、特権 EXEC モードで **show ospf neighbor** コマンドを使用します。

show ospf neighbor [***detail*** | *interface_name* [*nbr_router_id*]]

シンタックスの説明

detail	（オプション）指定したルータに関する詳細な情報を表示します。
interface_name	（オプション）ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	（オプション）隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 ospf neighbor** コマンドの出力例を示します。この例は、インターフェイスごとの OSPF ネイバー情報を表示する方法を示しています。

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
neighbor	非ブロードキャスト ネットワークに相互接続する OSPF ルータを設定します。
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf request-list** コマンドを使用します。

show ospf request-list *nbr_router_id interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。このインターフェイスからルータによって要求されたすべての LSA のリストを表示します。
nbr_router_id	隣接ルータのルータ ID。このネイバーからルータによって要求されたすべての LSA 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。

コマンドのモード

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 ospf request-list** コマンドの出力例を示します。

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

関連コマンド

コマンド	説明
show ospf retransmission-list	再送信されるのを待機しているすべての LSA のリストを表示します。

show ospf retransmission-list

再送信されるのを待機しているすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf retransmission-list** コマンドを使用します。

show ospf retransmission-list *nbr_router_id interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

nbr_router_id 引数を指定すると、この隣接ルータの、再送信されるのを待機しているすべての LSA のリストが表示されます。

interface_name 引数を指定すると、このインターフェイスの、再送信されるのを待機しているすべての LSA のリストが表示されます。

例

次に、**show ospf retransmission-list** コマンドの出力例を示します。例では、*nbr_router_id* 引数は 192.168.1.11 で、*if_name* 引数は outside です。

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

関連コマンド

コマンド	説明
show ospf request-list	ルータによって要求されたすべての LSA のリストを表示します。

show ospf summary-address

OSPF プロセスに対して設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、特権 EXEC モードで **show ospf summary-address** コマンドを使用します。

show ospf summary-address

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。

コマンドのモード

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 ospf summary-address** コマンドの出力例を示します。この例は、ID が 5 である OSPF プロセスに対してサマリー アドレスが設定される前に、すべてのサマリー アドレス再配布情報のリストを表示する方法を示しています。

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

関連コマンド

コマンド	説明
summary-address	OSPF の集約アドレスを作成します。

show ospf virtual-links

OSPF 仮想リンクのパラメータと現在の状態を表示するには、特権 EXEC モードで **show ospf virtual-links** コマンドを使用します。

show ospf virtual-links

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。

コマンドのモード

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 ospf virtual-links** コマンドの出力例を示します。

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

関連コマンド

コマンド	説明
area virtual-link	OSPF 仮想リンクを定義します。

show perfmon

セキュリティ アプライアンスのパフォーマンスに関する情報を表示するには、**show perfmon** コマンドを使用します。

show perfmon

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。

コマンドのモード

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)	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

このコマンドの出力は、Telnet コンソール セッションには表示されません。

perfmon コマンドを使用すると、セキュリティ アプライアンスのパフォーマンスを監視できます。**show perfmon** コマンドを使用すると、すぐに情報を表示できます。

例

次の例は、セキュリティ アプライアンスのパフォーマンスに関する情報を表示する方法を示しています。

```
hostname(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

関連コマンド

コマンド	説明
perfmon	詳細なパフォーマンス監視情報を表示します。

show pim df

ランデブー ポイント（RP）またはインターフェイスについて、双方向 DF の「勝者」を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim df** コマンドを使用します。

show pim df [**winner**] [*rp_address* | *if_name*]

シンタックスの説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
if_name	インターフェイスの物理名または論理名。
winner	（オプション）DF 選択の勝者をインターフェイスごと、RP ごとに表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、RP への勝者のメトリックも表示します。

例

次に、**show pim df** コマンドの出力例を示します。

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

グループからプロトコルへのマッピング テーブルを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim group-map** コマンドを使用します。

show pim group-map [***info-source***] [*group*]

シンタックスの説明

group	（オプション）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
info-source	（オプション）グループ範囲情報の情報源を表示します。

デフォルト

すべてのグループについて、グループからプロトコルへのマッピングを表示します。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、RP について、グループとプロトコルとのアドレス マッピングをすべて表示します。マッピングは、セキュリティ アプライアンス上でさまざまなクライアントからラーニングされます。

セキュリティ アプライアンスの PIM 実装は、さまざまな特殊エントリをマッピング テーブルで保持しています。Auto-RP グループ範囲は、希薄モード グループ範囲から明確に拒否されます。SSM グループ範囲も希薄モードには入りません。リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も、希薄モード グループ範囲から拒否されます。最後のエントリは、所定の RP で希薄モードに入っている残りすべてのグループを示します。

pim rp-address コマンドで複数の RP を設定した場合は、適切なグループ範囲が対応する RP とともに表示されます。

例

次に、**show pim group-map** コマンドの出力例を示します。

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

1 行目と 2 行目で、Auto-RP グループ範囲が希薄モード グループ範囲から明確に拒否されています。

3 行目では、リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も希薄モード グループ範囲から拒否されています。

4 行目では、PIM 送信元特定マルチキャスト（PIM-SSM）グループ範囲が 232.0.0.0/8 にマッピングされています。

最後のエントリは、残りすべてのグループが希薄モードに入って、RP 10.10.3.2 にマッピングされたことを示しています。

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。
pim rp-address	PIM ランデブー ポイント（RP）のアドレスを設定します。

show pim interface

PIM に関するインターフェイス固有の情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim interface** コマンドを使用します。

show pim interface [*if_name* | ***state-off*** | ***state-on***]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
state-off	（オプション）PIM がディセーブルになっているインターフェイスを表示します。
state-on	（オプション）PIM がイネーブルになっているインターフェイスを表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する PIM 情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、このコマンドの出力にあるネイバー数カラムでは、ネイバー数が実際の数よりも 1 つ多く表示されます。

例

次の例では、内部インターフェイスに関する PIM 情報を表示しています。

```
hostname# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show pim join-prune statistic

PIM の加入とプルーニングに関する集約的な統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim join-prune statistics** コマンドを使用します。

show pim join-prune statistics [*if_name*]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて、加入とプルーニングに関する統計情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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

PIM の加入とプルーニングに関する統計情報を消去するには、**clear pim counters** コマンドを使用します。

例

次に、**show pim join-prune statistic** コマンドの出力例を示します。

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim neighbor

PIM ネイバー テーブルに含まれているエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim neighbor** コマンドを使用します。

show pim neighbor [***count*** | ***detail***] [*interface*]

シンタックスの説明

interface	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
count	（オプション）PIM ネイバーの合計数、および各インターフェイスの PIM ネイバーの数を表示します。
detail	（オプション）upstream-detection hello オプションを通じてラーニングした、ネイバーの追加アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、このルータが PIM の hello メッセージを通じてラーニングした PIM ネイバーを特定するために使用します。また、このコマンドは、インターフェイスが指定ルータ（DR）であること、およびネイバーで双方向処理が可能になるタイミングも示します。

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、セキュリティ アプライアンス インターフェイスがこのコマンドの出力に表示されます。セキュリティ アプライアンスの IP アドレスは、アドレスの次にアスタリスク（*）を付けて示されています。

例

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

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show pim range-list

PIM の範囲リストの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim range-list** コマンドを使用します。

show pim range-list [*rp_address*]

シンタックスの説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、マルチキャスト転送モードからグループへのマッピングを特定するために使用します。出力には、この範囲のランデブー ポイント（RP）のアドレスも示されます（該当する場合）。

例

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

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

関連コマンド

コマンド	説明
show pim group-map	グループから PIM モードへのマッピング、およびアクティブな RP の情報を表示します。

show pim topology

PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology [*group*] [*source*]

シンタックスの説明

group	（オプション）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
source	（オプション）次のいずれかを指定できます。 • マルチキャスト送信元の名前。DNS の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • マルチキャスト送信元の IP アドレスこれは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

デフォルト

すべてのグループと送信元のトポロジ情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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

PIM トポロジ テーブルは、所定のグループのさまざまなエントリ、(*,G)、(S,G)、(S,G)RPT をそれぞれのインターフェイス リストとともに表示するために使用します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、インターネット グループ管理プロトコル（IGMP）などのローカル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

MRIB は、所定の (S,G) エントリについて、どのインターフェイスでデータ パケットを受け取る必要があるか、どのインターフェイスでデータ パケットを転送する必要があるかを示します。また、転送時にはマルチキャスト転送情報ベース（MFIB）テーブルを使用して、パケットごとの転送アクションを決定します。

（注） 転送情報を表示するには、**show mfib route** コマンドを使用します。

例

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

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside             15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside             15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside             15:57:16  fwd LI LH
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルを表示します。

show pim topology reserved

予約済みグループに関する PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology reserved** コマンドを使用します。

show pim topology reserved

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。

コマンドのモード

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
ユーザ EXEC または特権 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

なし。

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim topology route-count

PIM トポロジ テーブルのエントリの数を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology route-count** コマンドを使用します。

show pim topology route-count [***detail***]

シンタックスの説明

detail	（オプション）グループごとに、数に関する詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ EXEC または特権 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

このコマンドは、PIM トポロジ テーブルに保持されているエントリの数を表示します。エントリに関する詳細な情報を表示するには、**show pim topology** コマンドを使用します。

例

次に、**show pim topology route-count** コマンドの出力例を示します。

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim traffic

PIM トラフィックのカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim traffic** コマンドを使用します。

show pim traffic

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。

コマンドのモード

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
ユーザ EXEC または特権 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

PIM トラフィックのカウンタを消去するには、**clear pim counters** コマンドを使用します。

例

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

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                        0        9485
Hello                                    0        9485
Join-Prune                               0           0
Register                                 0           0
Register Stop                            0           0
Assert                                   0           0
Bidir DF Election                        0           0

Errors:
Malformed Packets                                    0
Bad Checksums                                        0
Send Errors                                          0
Packet Sent on Loopback Errors                       0
Packets Received on PIM-disabled Interface           0
Packets Received with Unknown PIM Version            0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタをクリアします。

show pim tunnel

PIM トンネル インターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim tunnels** コマンドを使用します。

show pim tunnels [*if_name*]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて PIM トンネル情報が表示されます。

コマンドのモード

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
ユーザ EXEC または特権 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

PIM レジスタ パケットは、仮想カプセル化トンネル インターフェイスを経由して、送信元の最初のホップ DR ルータから RP に送信されます。RP では、仮想カプセル化解除トンネルを使用して、PIM レジスタ パケットの受信インターフェイスを表現します。このコマンドは、両方のタイプのインターフェイスについてトンネル情報を表示します。

レジスタ トンネルは、（PIM レジスタ メッセージ内に）カプセル化された、送信元からのマルチキャスト パケットです。送信元は、共有ツリーを経由して、配布のために RP に送信されます。登録が適用されるのは、SM に対してのみです。SSM および 双方向 PIM には適用されません。

例

次に、**show pim tunnel** コマンドの出力例を示します。

```
hostname# show pim tunnel

Interface      RP Address Source Address


Encapstunnel0 10.1.1.1   10.1.1.1

Decapstunnel0 10.1.1.1   -
```

show priority-queue statistics

インターフェイスのプライオリティキューに関する統計情報を表示するには、特権 EXEC モードで **show priority-queue statistics** コマンドを使用します。

show priority-queue statistics [*interface-name*]

シンタックスの説明

interface-name	（オプション）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合は、すべての設定済みインターフェイスについてプライオリティキュー統計情報が表示されます。

コマンドのモード

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

次の例は、test というインターフェイスについて **show priority-queue statistics** コマンドを使用した場合のコマンド出力を示しています。この出力で、BE はベストエフォート キュー、LLQ は低遅延キューを表しています。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスからプライオリティキュー コンフィギュレーションを削除します。
clear priority-queue statistics	特定のインターフェイス、またはすべての設定済みインターフェイスに関するプライオリティキュー統計情報のカウンタを消去します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティキュー コンフィギュレーションを表示します。

show processes

セキュリティ アプライアンス上で動作しているプロセスのリストを表示するには、特権 EXEC モードで **show processes** コマンドを使用します。

show processes [cpu-hog | memory | internals]

デフォルト

デフォルトでは、このコマンドはセキュリティ アプライアンス上で動作しているプロセスを表示します。

コマンドのモード

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)	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 processes コマンドを使用すると、セキュリティ アプライアンス上で動作しているプロセスのリストを表示できます。

また、オプションの **cpu-hog** 引数を指定して実行すると、CPU を使用しているプロセスを特定するのに役立ちます。プロセスには、CPU を占有している期間が 100 ミリ秒を超えている場合、フラグが付けられます。**show process cpu-hog** コマンドを実行すると、次のカラムが表示されます。

- MAXHOG：CPU 占有実行の最長期間（ミリ秒単位）。
- NUMHOG：CPU 占有実行の回数。
- LASTHOG：最後の CPU 占有実行の期間（ミリ秒単位）。

プロセスは、数個の命令だけを必要とする軽量スレッドです。リスト内で、PC はプログラム カウンタ、SP はスタック ポインタ、STATE はスレッド キューのアドレス、Runtime はスレッドが実行されている（CPU クロックのサイクルに基づく）時間（ミリ秒）、SBASE はスタックのベース アドレス、Stack はスタックの現在使用されているバイト数と合計サイズであり、Process はスレッドの機能を示します。

オプションの **memory** 引数を指定すると、各プロセスによって割り当てられたメモリが表示されます。この情報は、プロセスによるメモリ使用状況を追跡するのに役立ちます。

オプションの **internals** 引数を指定すると、起動されたコールの数とギブアップの数が表示されます。Invoked は、スケジューラがプロセスを起動した（実行した）回数です。Giveups は、プロセスが CPU をスケジューラに返還した回数です。

例

次の例は、セキュリティ アプライアンス上で動作しているプロセスのリストを表示する方法を示しています。

```
hostname(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

hostname(config)# show processes cpu

    MAXHOG              NUMHOG              LASTHOG              Process
--------------     ---------------     ---------------       ---------
      7720                  4                 110              Dispatch Unit
      7870                331                1010              Checkheaps
(other lines deleted for brevity)
      6170                  1                6170              CTM message handle

hostname(config)# show processes memory

-------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
-------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)

hostname# sho proc internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

show reload

セキュリティ アプライアンスのリロードのステータスを表示するには、特権 EXEC モードで ***show reload*** コマンドを使用します。

show reload

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。

コマンドのモード

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

このコマンドに使用上のガイドラインはありません。

例

次の例は、リロードが 4 月 20 日、日曜日の午前 0 時（夜の 12 時）にスケジューリングされていることを示しています。

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

関連コマンド

コマンド	説明
reload	コンフィギュレーションをリブートおよびリロードします。

show resource types

セキュリティ アプライアンスが使用状況の追跡対象にしているリソース タイプを表示するには、特権 EXEC モードで **show resource types** コマンドを使用します。

show resource types

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。

コマンドのモード

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

次の例では、リソース タイプを表示しています。

```
hostname# show resource types

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  IPSec           IPSec Mgmt Tunnels
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

関連コマンド

コマンド	説明
clear resource usage	リソース使用状況の統計情報を消去します。
context	セキュリティ コンテキストを追加します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

show resource usage

セキュリティ アプライアンスまたはマルチ モードの各コンテキストのリソース使用状況を表示するには、特権 EXEC モードで **show resource usage** コマンドを使用します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**]
[**resource** {*resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

シンタックスの説明

context *context_name*	(マルチ モードのみ) 統計情報を表示するコンテキストの名前を指定します。すべてのコンテキストを対象にするには、**all** を指定します。セキュリティ アプライアンスは、各コンテキストのリソース使用状況を一覧表示します。
count_threshold	使用回数を設定します。この回数以上に使用されているリソースが表示の対象になります。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*current_threshold* は現在の使用状況に適用されます。 **（注）** すべてのリソースを表示するには、*count_threshold* を **0** に設定します。
counter *counter_name*	次のカウンタ タイプの数を表示します。 • **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。 • **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後に消去された時点から計測されます。 • **all**：(デフォルト) すべての統計情報を表示します。
resource *resource_name*	特定のリソースの使用状況を表示します。すべてのリソースを対象にするには、***all***（デフォルト）を指定します。リソースには、次のタイプがあります。 • **conns**：任意の 2 ホスト間の TCP 接続または UDP 接続（1 つのホストと、その他の複数のホストとの接続を含む）。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **ipsec**：(シングルモードのみ) IPSec セッション。 • **ssh**：SSH セッション。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	(マルチ モードのみ) すべてのコンテキストの合算使用状況を表示します。
system	(マルチ モードのみ) すべてのコンテキストの合算使用状況を表示します。ただし、コンテキストの合算制限値ではなくシステムのリソース制限値を表示します。
top *n*	(マルチ モードのみ) 指定したリソースの上位 *n* 人のユーザのコンテキストを表示します。このオプションでは、**resource all** ではなくリソース タイプを 1 つのみ指定する必要があります。

デフォルト

マルチ コンテキスト モードでは、デフォルト コンテキストは **all** です。すべてのコンテキストのリソース使用状況が表示されます。シングルモードの場合、コンテキスト名は無視され、出力では「context」は「System」として表示されます。

デフォルトのリソース名は、**all** です。すべてのリソース タイプが表示されます。

デフォルトのカウンタ名は、**all** です。すべての統計情報が表示されます。

デフォルトのカウントしきい値は、**1** です。

コマンドのモード

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 resource usage context** コマンドの出力例を示します。この例では、admin コンテキストのリソース使用状況を表示しています。

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Context
Telnet                      1            1          5    admin
Conns                      44           55        N/A    admin
Hosts                      45           56        N/A    admin
```

次に、**show resource usage summary** コマンドの出力例を示します。この例では、すべてのコンテキストとすべてのリソースのリソース使用状況が表示されます。ここでは、6 コンテキスト分の制限値が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit    Context
Telnet                      3            5         30    Summary
SSH                         5            7         30    Summary
Conns                      40           55        N/A    Summary
Hosts                      44           56        N/A    Summary
```

次に、**show resource usage summary** コマンドの出力例を示します。この例では、25 コンテキスト分の制限値が表示されています。Telnet 接続と SSH 接続のコンテキスト制限値は 1 コンテキストあたり 5 であるため、合算の制限値は 125 になります。システム制限値は 100 であるため、システム制限値が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit    Context
Telnet                      1            1      100[S]  Summary
SSH                         2            2      100[S]  Summary
Conns                      56           90        N/A    Summary
Hosts                      89          102        N/A    Summary
S = System limit: Combined context limits exceed the system limit; the system limit is
shown.
```

次に、**show resource usage system** コマンドの出力例を示します。この例では、すべてのコンテキストのリソース使用状況が表示されますが、合算のコンテキスト制限値ではなくシステム制限値が表示されています。

```
hostname# show resource usage system

Resource                Current         Peak      Limit    Context
Telnet                        3            5        100    System
SSH                           5            7        100    System
Conns                        40           55        N/A    System
Hosts                        44           56        N/A    System
```

関連コマンド

コマンド	説明
clear resource usage	リソース使用状況の統計情報を消去します。
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。

show route

インターフェイスのデフォルト ルートまたはスタティック ルートを表示するには、特権 EXEC モードで **show route** コマンドを使用します。

show route [*interface_name ip_address netmask gateway_ip*]

シンタックスの説明

gateway_ip	（オプション）ゲートウェイ ルータの IP アドレス（このルートのネクスト ホップ アドレス）。
interface_name	（オプション）内部または外部のネットワーク インターフェイス名。
ip_address	（オプション）内部または外部のネットワーク IP アドレス。
netmask	（オプション）*ip_address* に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 route** コマンドの出力例を示します。

```
hostname(config)# show route
C    10.30.10.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show running-config route	設定されているルートを表示します。

show run fips

FIPS システムの位置やシステム連絡先などを確認するには、**show run fips** コマンドを使用します。

show run fips

シンタックスの説明

fips	FIPS 140-2 準拠情報

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。

コマンドのモード

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(4)	このコマンドが導入されました。

使用上のガイドライン

show run fips コマンドは、システム コンフィギュレーションに関する情報を表示します。

例

```
sw8-ASA(config)# show run fips
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
service internal	通常は表示されない、条件付きコマンドへのアクセスを許可します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

show running-config

セキュリティ アプライアンス上で実行されているコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**all**] [*command*]

シンタックスの説明

all	デフォルト値を含めて、実行コンフィギュレーション全体を表示します。
command	特定のコマンドに関連付けられているコンフィギュレーションを表示します。

デフォルト

引数もキーワードも指定しない場合は、デフォルト以外に設定されているセキュリティ アプライアンス コンフィギュレーション全体が表示されます。

コマンドのモード

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)	このコマンドが変更されました。

使用上のガイドライン

show running-config コマンドは、セキュリティ アプライアンス上の現在の実行コンフィギュレーションを表示します。

running-config キーワードは、**show running-config** コマンド内だけで使用できます。このキーワードを **no** および **clear** とともに使用することはできません。また、スタンドアロン コマンドとして使用することもできません。CLI ではサポートされないコマンドとして処理されます。**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

（注） デバイス　マネージャのコマンドを使用してセキュリティ　アプライアンスに接続するかセキュリティ アプライアンスを設定した後は、デバイス マネージャのコマンドがコンフィギュレーションに表示されます。

例

次の例は、セキュリティ アプライアンス上で実行されているコンフィギュレーションを表示する方法を示しています。

```
hostname# show running-config
: Saved
:
XXX Version X.X(X)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
```

```
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

関連コマンド

コマンド	説明
configure	セキュリティ アプライアンスを端末から設定します。

show running-config aaa

実行コンフィギュレーションの AAA コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa** コマンドを使用します。

show running-config aaa [***accounting*** | ***authentication*** | ***authorization*** | ***mac-exempt*** | ***proxy-limit***]

シンタックスの説明

accounting	（オプション）アカウンティング関連の AAA コンフィギュレーションを表示します。
authentication	（オプション）認証関連の AAA コンフィギュレーションを表示します。
authorization	（オプション）認可関連の AAA コンフィギュレーションを表示します。
mac-exempt	（オプション）MAC アドレス免除の AAA コンフィギュレーションを表示します。
proxy-limit	（オプション）ユーザ 1 人あたりに許可されている同時プロキシ接続の数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config aaa** コマンドの出力例を示します。

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure
radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
```

関連コマンド

コマンド	説明
aaa authentication match	アクセスリストによって識別されるトラフィックに対する認証をイネーブルにします。
aaa authorization match	アクセスリストによって識別されるトラフィックに対する認可をイネーブルにします。
aaa accounting match	アクセスリストによって識別されるトラフィックに対するアカウンティングをイネーブルにします。
aaa mac-exempt	認証と認可を免除される MAC アドレスの事前定義済みリストを使用することを指定します。
aaa proxy-limit	ユーザ 1 人あたりに許可する同時プロキシ接続の最大数を設定して、uauth セッション制限を設定します。

show running-config aaa-server

AAA サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show running-config [**all**] **aaa-server** [*server-tag*] [(*interface-name*)] [**host** *hostname*]

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。
host *hostname*	（オプション）AAA サーバ統計情報の表示対象となる、特定のホストのシンボリック名または IP アドレス。
(interface-name)	（オプション）AAA サーバが常駐するネットワーク インターフェイス。
server-tag	（オプション）サーバグループのシンボリック名。

デフォルト

server-tag 値を省略すると、すべての AAA サーバのコンフィギュレーションが表示されます。

コマンドのモード

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)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドは、特定のサーバグループの設定を表示するために使用します。明示的に設定されている値に加えてデフォルト値も表示するには、**all** パラメータを使用します。

例

デフォルト AAA サーバグループの実行コンフィギュレーションを表示するには、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
```

関連コマンド

コマンド	説明
show aaa-server	AAA サーバの統計情報を表示します。
clear configure aaa-server	AAA サーバのコンフィギュレーションを消去します。

show running-config aaa-server host

特定のサーバの AAA サーバ統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

シンタックスの説明

all	(オプション) 実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。
server-tag	サーバグループのシンボリック名。

デフォルト

default キーワードを省略すると、明示的に設定されているコンフィギュレーション値のみが表示され、デフォルト値は表示されません。

コマンドのモード

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	•	•	—	—	•
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)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドは、特定のサーバグループの統計情報を表示するために使用します。明示的に設定されている値に加えてデフォルト値も表示するには、default パラメータを使用します。

例

サーバグループ svrgrp1 の実行コンフィギュレーションを表示するには、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server svrgrp1
```

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、またはプロトコルの AAA サーバ設定を表示します。
clear configure aaa	すべてのグループのすべての AAA サーバの設定を削除します。

show running-config access-group

アクセス グループの情報を表示するには、特権 EXEC モードで **show running-config access-group** コマンドを使用します。

show running-config access-group

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。

コマンドのモード

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 running-config access-group** コマンドの出力例を示します。

```
hostname# show running-config access-group
access-group 100 in interface outside
```

関連コマンド

コマンド	説明
access-group	アクセスリストをインターフェイスにバインドします。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。

show running-config access-list

セキュリティ アプライアンス上で実行されているアクセスリストのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config access-list** コマンドを使用します。

show running-config [***default***] **access-list** [**alert-interval** | **deny-flow-max**]

show running-config [***default***] **access-list** *id* [*saddr_ip*]

シンタックスの説明

alert-interval	syslog メッセージ 106001 を生成する警告間隔を表示します。このメッセージは、システムが拒否フローの最大数に達したことを警告するものです。
deny-flow-max	作成できる同時拒否フローの最大数を表示します。
id	表示するアクセスリストを指定します。
saddr_ip	指定した送信元 IP アドレスを保持しているアクセスリスト要素を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

show running-config access-list コマンドを使用すると、セキュリティ アプライアンス上の現在のアクセスリスト実行コンフィギュレーションを表示できます。

例

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

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

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。
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。
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 alias

コンフィギュレーションに含まれている、デュアル NAT コマンドで使用する重複アドレスを表示するには、特権 EXEC モードで **show running-config alias** コマンドを使用します。

show running-config alias {*interface_name*}

シンタックスの説明

interface_name	destination_ip が上書きする、内部ネットワーク インターフェイス名。

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。

コマンドのモード

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。

例

次の例は、エイリアス情報を表示する方法を示しています。

```
hostname# show running-config alias
```

関連コマンド

コマンド	説明
alias	エイリアスを作成します。
clear configure alias	エイリアスを削除します。

show running-config arp

arp コマンドで作成し、実行コンフィギュレーションに含まれているスタティック ARP エントリを表示するには、特権 EXEC モードで **show running-config arp** コマンドを使用します。

show running-config 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。

コマンドのモード

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	このコマンドが導入されました。

例

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

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

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。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show running-config arp timeout

実行コンフィギュレーションの ARP タイムアウト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp timeout** コマンドを使用します。

show running-config arp timeout

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。

コマンドのモード

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 arp timeout** から変更されました。

例

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

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

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 timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの期間を設定します。
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。
show arp statistics	ARP 統計情報を表示します。

show running-config arp-inspection

実行コンフィギュレーションの ARP 検査コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp-inspection** コマンドを使用します。

show running-config 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。

コマンドのモード

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 arp timeout** から変更されました。

例

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

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable no-flood
```

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 configure arp-inspection	ARP 検査のコンフィギュレーションを消去します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。

show running-config asdm

実行コンフィギュレーションに含まれている **asdm** コマンドを表示するには、特権 EXEC モードで **show running-config asdm** コマンドを使用します。

show running-config asdm [**group** | **location**]

シンタックスの説明

group	（オプション）実行コンフィギュレーションに含まれている **asdm group** コマンドのみを表示します。
location	（オプション）実行コンフィギュレーションに含まれている **asdm location** コマンドのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config pdm** コマンドから **show running-config asdm** コマンドに変更されました。

使用上のガイドライン

asdm コマンドをコンフィギュレーションから削除するには、**clear configure asdm** コマンドを使用します。

（注）　マルチ コンテキスト モードで動作しているセキュリティ アプライアンスでは、**show running-config asdm group** コマンドと **show running-config asdm location** コマンドを使用できるのはシステム実行スペース内のみです。

例

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

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。

show running-config auth-prompt

現在の認証プロンプト チャレンジ テキストを表示するには、グローバル コンフィギュレーション モードで show running-config auth-prompt コマンドを使用します。

show running-config [default] auth-prompt

シンタックスの説明

default	（オプション）デフォルトの認証プロンプト チャレンジ テキストを表示します。

デフォルト

設定されている認証プロンプト チャレンジ テキストを表示します。

コマンドのモード

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、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

show running-config auth-prompt コマンドは、**auth-prompt** コマンドで認証プロンプトを設定した後に、現在のプロンプト テキストを表示するために使用します。

例

次に、**show running-config auth-prompt** コマンドの出力例を示します。

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
clear configure auth-prompt	ユーザ認可プロンプトをデフォルト値にリセットします。

show running-config banner

指定したバナー、およびそのバナーに設定されているすべての行を表示するには、特権 EXEC モードで **show running-config banner** コマンドを使用します。

show running-config banner [**exec** | **login** | **motd**]

シンタックスの説明

exec	（オプション）イネーブル プロンプトを表示する前にバナーを表示します。
login	（オプション）ユーザが Telnet を使用してセキュリティ アプライアンスにアクセスしたときに、パスワード ログイン プロンプトを表示する前にバナーを表示します。
motd	（オプション）「今日のお知らせ」バナーを表示します。

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。

コマンドのモード

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)	***running-config*** キーワードが追加されました。

使用上のガイドライン

show running-config banner コマンドは、キーワードで指定したバナー、およびそのバナーに設定されているすべての行を表示します。キーワードを指定しない場合は、すべてのバナーが表示されます。

例

次の例は、「今日のお知らせ」（motd）バナーを表示する方法を示しています。

```
hostname# show running-config banner motd
```

関連コマンド

コマンド	説明
banner	バナーを作成します。
clear configure banner	バナーを削除します。

show running-config class-map

クラスマップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config class-map** コマンドを使用します。

show running-config [***all***] **class-map** [*class_map_name*]

シンタックスの説明

all	（オプション）デフォルト値を含めて、実行されているすべてのクラスマップ コンフィギュレーションを表示します。
class_map_name	（オプション）クラスマップ名のテキスト。テキストの長さは、40 文字までです。

デフォルト

match any コマンドを 1 つだけ含んでいる **class-map class-default** コマンドが、デフォルトのクラスマップです。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config class-map** コマンドの出力例を示します。

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。

show running-config clock

実行コンフィギュレーションのクロック コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config clock** コマンドを使用します。

show running-config [**all**] **clock**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **clock** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

all キーワードを指定した場合は、**clock summer-time** コマンドの正確な日時もオフセットのデフォルト設定（オフセットを設定しなかった場合）とともに表示されます。

例

次に、**show running-config clock** コマンドの出力例を示します。**clock summer-time** コマンドのみ設定されていました。

```
hostname# show running-config clock
clock summer-time EDT recurring
```

次に、**show running-config all clock** コマンドの出力例を示します。設定されていない **clock timezone** コマンドについてはデフォルト設定が表示され、**clock summer-time** コマンドについては詳細な情報が表示されています。

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。

show running-config command-alias

設定されているコマンド エイリアスを表示するには、特権 EXEC モードで ***show running-config command-alias*** コマンドを使用します。

show running-config [all] command-alias

シンタックスの説明

all	（オプション）デフォルト値を含めて、設定されているすべてのコマンド エイリアスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

all キーワードを入力しない場合は、デフォルト以外のコマンド エイリアスのみが表示されます。

例

次の例では、デフォルト値を「含めて」、セキュリティ アプライアンス上に設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

次の例では、デフォルト値を「除いて」、セキュリティ アプライアンス上に設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
clear configure command-alias	デフォルト以外のコマンド エイリアスをすべて削除します。

show running-config console timeout

コンソール接続のタイムアウト値を表示するには、特権 EXEC モードで **show running-config console timeout** コマンドを使用します。

show running-config console timeout

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。

コマンドのモード

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)	**running-config** キーワードが追加されました。

例

次の例は、コンソール接続のタイムアウト設定を表示する方法を示しています。

```
hostname# show running-config console timeout
console timeout 0
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
clear configure console	コンソール接続の設定をデフォルトにリセットします。

show running-config context

システム実行スペースのコンテキスト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config context** コマンドを使用します。

show running-config context

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。

コマンドのモード

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	このコマンドが導入されました。

例

次に、**show running-config context** コマンドの出力例を示します。

```
hostname# show running-config context

admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url flash:/admin.cfg
!

context A
  allocate-interface GigabitEthernet0/1
  config-url flash:/A.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。
allocate-interface	コンテキストにインターフェイスを割り当てます。
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。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。

show running-config crypto

IPSec、暗号マップ、ダイナミック暗号マップ、および ISAKMP を含めた暗号コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto** コマンドを使用します。

show running-config crypto

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

特権 EXEC モードで入力した次の例では、すべての暗号コンフィギュレーション情報を表示しています。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto dynamic-map

ダイナミック暗号マップを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto dynamic-map** コマンドを使用します。

show running-config crypto dynamic-map

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

グローバル コンフィギュレーション モードで入力した次の例では、ダイナミック暗号マップに関するすべてのコンフィギュレーション情報を表示しています。

```
hostname(config)# show running-config crypto dynamic-map

Crypto Map Template "dyn1" 10

        access-list 152 permit ip host 172.21.114.67 any
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={ tauth, t1, }
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto ipsec

IPSec コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto ipsec** コマンドを使用します。

show running-config crypto ipsec

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

グローバル コンフィギュレーション モードで発行した次の例では、IPSec コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto isakmp** コマンドを使用します。

show running-config crypto isakmp

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname<config># show running-config crypto isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname<config>#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto map

すべての暗号マップのすべてのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto map** コマンドを使用します。

show running-config crypto map

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	—	—
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

特権 EXEC モードで入力した次の例では、すべての暗号マップのすべてのコンフィギュレーション情報を表示しています。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
hostname#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config dhcpd

DHCP コンフィギュレーションを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config dhcpd** コマンドを使用します。

show running-config *dhcpd*

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。

コマンドのモード

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 dhcpd** コマンドから **show running-config dhcpd** コマンドに変更されました。

使用上のガイドライン

show running-config dhcpd コマンドは、実行コンフィギュレーションに入力されている DHCP のコマンドを表示します。DHCP のバインディング、状態、および統計情報を表示するには、**show dhcpd** コマンドを使用します。

例

次に、**show running-config dhcpd** コマンドの出力例を示します。

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
debug dhcpd	DHCP サーバに対するデバッグ情報を表示します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

show running-config dhcprelay

現在の DHCP リレー エージェント コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dhcprelay** コマンドを使用します。

show running-config *dhcprelay*

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。

コマンドのモード

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。

使用上のガイドライン

show running-config dhcprelay コマンドは、現在の DHCP リレー エージェント コンフィギュレーションを表示します。DHCP リレー エージェントのパケット統計情報を表示するには、**show dhcprelay statistics** コマンドを使用します。

例

次に、**show running-config dhcprelay** コマンドの出力例を示します。

```
hostname(config)# show running-config dhcprelay

dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。

show running-config dns

実行コンフィギュレーションの DNS コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dns** コマンドを使用します。

show running-config dns

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。

コマンドのモード

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 running-config dns** コマンドの出力例を示します。

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受け取らなかった場合に、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

show running-config domain-name

実行コンフィギュレーションのドメイン名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config domain-name** コマンドを使用します。

show running-config domain-name

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。

コマンドのモード

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 domain-name** から変更されました。

例

次に、**show running-config domain-name** コマンドの出力例を示します。

```
hostname# show running-config domain-name
example.com
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。

show running-config enable

暗号化されたイネーブル パスワードを表示するには、特権 EXEC モードで **show running-config enable** コマンドを使用します。

show running-config enable

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。

コマンドのモード

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 enable** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは ***encrypted*** キーワードとともに表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config enable** コマンドの出力例を示します。

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

関連コマンド

コマンド	説明
disable	特権 EXEC モードを終了します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。

show running-config established

確立済みの接続に基づいて許可されている着信接続を表示するには、特権 EXEC モードで **show running-config established** コマンドを使用します。

show running-config established

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。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

この例は、確立済みの接続に基づいて許可されている着信接続を表示する方法を示しています。

```
hostname# show running-config established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
clear configure established	確立されたコマンドをすべて削除します。

show running-config failover

コンフィギュレーションに含まれている **failover** コマンドを表示するには、特権 EXEC モードで **show running-config failover** コマンドを使用します。

show running-config [*all*] **failover**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての failover コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config failover コマンドは、実行コンフィギュレーションに含まれている **failover** コマンドを表示します。**monitor-interface** コマンドおよび **join-failover-group** コマンドは表示しません。

例

次の例では、フェールオーバーを設定する前のデフォルト フェールオーバー コンフィギュレーションを表示しています。

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
hostname#
```

関連コマンド

コマンド	説明
show failover	フェールオーバーの状態と統計情報を表示します。

show running-config filter

フィルタリング コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config filter** コマンドを使用します。

show running-config filter

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config filter コマンドは、セキュリティ アプライアンスのフィルタリング コンフィギュレーションを表示します。

例

次に、**show running-config filter** コマンドの出力例を示します。セキュリティ アプライアンスのフィルタリング コンフィギュレーションが表示されています。

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

この例では、アドレス 10.86.194.170 について、ポート 80 で ActiveX フィルタリングがイネーブルになっています。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。

show running-config fips

セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示するには、**show running-config fips** コマンドを使用します。

show running-config fips

シンタックスの説明

fips	FIPS-2 準拠情報

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。

コマンドのモード

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(4)	このコマンドが導入されました。

使用上のガイドライン

show running-config fips コマンドを使用すると、現在の実行 FIPS コンフィギュレーションを表示できます。**running-config** キーワードは、**show running-config fips** コマンド内だけで使用します。このキーワードを no または clear とともに使用することはできません。また、スタンドアロン コマンドとして使用することもできません。そのような使用方法はサポートされていません。また、**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

例

```
sw8-ASA(config)# show running-config fips
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。

show running-config fragment

フラグメント データベースの現在のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config fragment** コマンドを使用します。

show running-config fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

インターフェイスが指定されていなければ、このコマンドはすべてのインターフェイスに適用されます。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

show running-config fragment コマンドは、フラグメント データベースの現在のコンフィギュレーションを表示します。インターフェイス名が指定されていれば、指定したインターフェイスに常駐するデータベースの情報だけを表示します。インターフェイス名が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

show running-config fragment コマンドは、次の情報を表示するために使用します。

- Size：**size** キーワードで設定されるパケットの最大数。この値は、インターフェイス上で許容されるフラグメントの最大数です。
- Chain：**chain** キーワードで設定される 1 つのパケットのフラグメントの最大数。
- Timeout：**timeout** キーワードで設定される最大秒数。これは、フラグメント化されたパケット全体が到着するのを待つ最大秒数です。タイマーは、パケットの最初のフラグメントが到着すると始動します。指定した秒数以内にパケットのすべてのフラグメントが到着しない場合、それまでに受信したパケット フラグメントはすべて廃棄されます。

例

次の例は、すべてのインターフェイス上のフラグメント データベースの状態を表示する方法を示しています。

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次の例は、名前が「outside」で始まるインターフェイス上にあるフラグメント データベースの状態を表示する方法を示しています。

（注）　この例では、「outside1」、「outside2」、および「outside3」という名前のインターフェイスが表示されています。

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次の例は、「outside1」というインターフェイス上にあるフラグメント データベースについてのみ、状態を表示する方法を示しています。

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。

show running-config ftp-map

設定済みの FTP マップを表示するには、特権 EXEC モードで **show running-config ftp-map** コマンドを使用します。

show running-config ftp-map *map_name*

シンタックスの説明.

map_name	指定した FTP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config ftp-map コマンドは、設定済みの FTP マップを表示します。

例

次に、**show running-config ftp-map** コマンドの出力例を示します。

```
hostname# show running-config ftp-map ftp-policy
!
ftp-map ftp-policy
request-command deny put stou appe
!
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
request-command deny	禁止する FTP コマンドを指定します。

show running-config ftp mode

FTP に関して設定されているクライアント モードを表示するには、特権 EXEC モードで **show running-config ftp mode** コマンドを使用します。

show running-config ftp mode

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config ftp mode コマンドは、FTP サーバにアクセスするときにセキュリティ アプライアンスが使用するクライアント モードを表示します。

例

次に、**show running-config ftp-mode** コマンドの出力例を示します。

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

関連コマンド

コマンド	説明
copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
ftp mode passive	FTP サーバにアクセスするときにセキュリティ アプライアンスが使用する FTP クライアント モードを設定します。

show running-config global

コンフィギュレーションに含まれている **global** コマンドを表示するには、特権 EXEC モードで **show running-config global** コマンドを使用します。

show running-config global

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。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config global** コマンドの出力例を示します。

```
hostname# show running-config global
global (outside1) 10 interface
```

関連コマンド

コマンド	説明
clear configure global	コンフィギュレーションから **global** コマンドを削除します。
global	グローバル アドレス プールに対してエントリを作成します。

show running-config group-delimiter

トンネルのネゴシエーション中に受信したユーザ名に基づいてグループ名を解析するときに使用する、現在のデリミタを表示するには、グローバル コンフィギュレーション モードで **show running-config group-delimiter** コマンドを使用します。

show running-config group-delimiter

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。

コマンドのモード

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

このコマンドは、現在設定されているグループデリミタを表示するために使用します。

例

次の例は、**show running-config group-delimiter** コマンドおよびその出力を示しています。

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

関連コマンド

コマンド	説明
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。

show running-config group-policy

特定のグループポリシーの実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config group-policy** コマンドを使用するときに、グループポリシーの名前を付加します。すべてのグループポリシーの実行コンフィギュレーションを表示するには、特定のグループポリシーを指定せずにこのコマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**default** キーワードを使用します。

show running-config [default] group-policy [*name***]**

シンタックスの説明

default	実行コンフィギュレーションを、デフォルト値を含めて表示します。
name	グループポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループポリシーの実行コンフィギュレーションをデフォルト値を含めて表示する方法を示しています。

```
hostname# show running-config default group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループポリシーを作成、編集、または削除します。
group-policy attributes	指定したグループポリシーの AVP を設定できるグループポリシー アトリビュート モードに入ります。
clear config group-policy	特定のグループポリシーまたはすべてのグループポリシーのコンフィギュレーションを削除します。

show running-config gtp-map

設定済みの GTP マップを表示するには、特権 EXEC モードで **show running-config gtp-map** コマンドを使用します。

show running-config gtp-map *map_name*

シンタックスの説明.

map_name	指定した GTP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config gtp-map コマンドは、設定済みの GTP マップを表示します。

例

次に、**show running-config gtp-map** コマンドの出力例を示します。

```
hostname# show running-config gtp-map gtp-policy
!
gtp-map gtp-policy
 request-queue 300
 message-length min 20 max 300
 drop message 20
 tunnel-limit 10000
!
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

show running-config http

現在の一連の設定済み http コマンドを表示するには、特権 EXEC モードで **show running-config http** コマンドを使用します。

show running-config http

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

例

次の出力例は、**show running-config http** コマンドを使用する方法を示しています。

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

関連コマンド

コマンド	説明
clear http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。

show running-config http-map

設定済みの HTTP マップを表示するには、特権 EXEC モードで **show running-config http-map** コマンドを使用します。

show running-config http-map *map_name*

シンタックスの説明.

map_name	指定した HTTP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config http-map コマンドは、設定済みの HTTP マップを表示します。

例

次に、**show running-config http-map** コマンドの出力例を示します。

```
hostname# show running-config http-map http-policy
!
http-map http-policy
content-length min 100 max 2000 action reset log
content-type-verification match-req-rsp reset log
max-header-length request bytes 100 action log reset
max-uri-length 100 action reset log
!
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

show running-config icmp

ICMP トラフィックに対して設定されているアクセス規則を表示するには、特権 EXEC モードで **show running-config icmp** コマンドを使用します。

show running-config icmp *map_name*

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config icmp コマンドは、ICMP トラフィックに対して設定されているアクセス規則を表示します。

例

次に、**show running-config icmp** コマンドの出力例を示します。

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show running-config imap4s

IMAP4S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config imap4s** コマンドを使用します。

show running-config [all] imap4s

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。

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。

コマンドのモード

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	•	—	•	—	—

例

次に、**show running-config imap4s** コマンドの出力例を示します。

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
imap4s	IMAP4S 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config interface

実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config interface** コマンドを使用します。

show running-config [**all**] **interface** [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **interface** コマンドを表示します。
interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ　コンテキスト　モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンドのモード

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

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。

例

次に、**show running-config interface** コマンドの出力例を示します。この例では、すべてのインターフェイスの実行コンフィギュレーションを表示しています。GigabitEthernet0/2 インターフェイスと GigabitEthernet0/3 インターフェイスはまだ設定されていないため、デフォルトのコンフィギュレーションが表示されます。Management0/0 インターフェイスについても、デフォルトの設定が表示されています。

```
formula_1# show running-config interface
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 security-level 0
 no ip address
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイス コンフィギュレーションを消去します。
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。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show running-config ip address

実行コンフィギュレーションの IP アドレス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip address** コマンドを使用します。

show running-config ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスの IP アドレス コンフィギュレーションが表示されます。

コマンドのモード

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

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内でのみ指定できます。

透過ファイアウォール モードの場合は、インターフェイスを指定しないでください。このコマンドは、管理 IP アドレスのみを表示するものであり、透過ファイアウォールではインターフェイスに IP アドレスが関連付けられていないためです。

このコマンドの表示内容では、**nameif** コマンドと **security-level** コマンドのコンフィギュレーションも示されます。

例

次に、**show running-config ip address** コマンドの出力例を示します。

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションを消去します。
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。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config ip audit attack

実行コンフィギュレーションの **ip audit attack** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit attack** コマンドを使用します。

show running-config ip audit attack

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。

コマンドのモード

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 ip audit attack** から変更されました。

例

次に、**show running-config ip audit attack** コマンドの出力例を示します。

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit info

実行コンフィギュレーションの **ip audit info** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit info** コマンドを使用します。

show running-config ip audit info

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。

コマンドのモード

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 ip audit info** から変更されました。

例

次に、**show running-config ip audit info** コマンドの出力例を示します。

```
hostname# show running-config ip audit info
ip audit info action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit interface

実行コンフィギュレーションの **ip audit interface** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit interface** コマンドを使用します。

show running-config ip audit interface [*interface_name*]

シンタックスの説明

interface_name	（オプション）インターフェイス名を指定します。

デフォルト

インターフェイス名を指定しない場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンドのモード

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 ip audit interface** から変更されました。

例

次に、**show running-config ip audit interface** コマンドの出力例を示します。

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit name

実行コンフィギュレーションの **ip audit name** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit name** コマンドを使用します。

show running-config ip audit name [*name* [***info*** | ***attack***]]

シンタックスの説明

attack	（オプション）攻撃シグニチャに対する名前付き監査ポリシーのコンフィギュレーションを表示します。
info	（オプション）情報シグニチャに対する名前付き監査ポリシーのコンフィギュレーションを表示します。
name	（オプション）**ip audit name** コマンドを使用して作成した監査ポリシー名のコンフィギュレーションを表示します。

デフォルト

名前を指定しない場合は、すべての監査ポリシーのコンフィギュレーションが表示されます。

コマンドのモード

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 ip audit name** から変更されました。

例

次に、**show running-config ip audit name** コマンドの出力例を示します。

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit signature

実行コンフィギュレーションの **ip audit signature** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit signature** コマンドを使用します。

show running-config ip audit signature [*signature_number*]

シンタックスの説明

signature_number	（オプション）このシグニチャ番号に対応するコンフィギュレーションが存在する場合は、表示します。サポートされているシグニチャのリストについては、**ip audit signature** コマンドを参照してください。

デフォルト

番号を指定しない場合は、すべてのシグニチャのコンフィギュレーションが表示されます。

コマンドのモード

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 ip audit signature** から変更されました。

例

次に、**show running-config ip audit signature** コマンドの出力例を示します。

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip local pool

IP アドレス プールを表示するには、特権 EXEC モードで **show running-config ip local pool** コマンドを使用します。

show running-config ip local pool [*poolname*]

シンタックスの説明

poolname	（オプション）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ip local pool** コマンドの出力例を示します。

```
hostname(config)# show running-config ip local pool firstpool

Pool            Begin           End             Mask            Free    In use
firstpool               10.20.30.40     10.20.30.50     255.255.255.0      11
    0
Available Addresses:
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての ip ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

show running-config ip verify reverse-path

実行コンフィギュレーションの **ip verify reverse-path** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip verify reverse-path** コマンドを使用します。

show running-config ip verify reverse-path [interface *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）指定したインターフェイスのコンフィギュレーションを表示します。

デフォルト

このコマンドは、すべてのインターフェイスのコンフィギュレーションを表示します。

コマンドのモード

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 ip verify reverse-path** から変更されました。

例

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

```
hostname# show running-config ip verify reverse-path
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。

show running-config ipv6

実行コンフィギュレーションに含まれている IPv6 のコマンドを表示するには、特権 EXEC モードで **show running-config ipv6** コマンドを使用します。

show running-config [**all**] **ipv6**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、実行コンフィギュレーションに含まれているすべての **ipv6** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config ipv6** コマンドの出力例を示します。

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

関連コマンド

コマンド	説明
debug ipv6	IPv6 デバッグ メッセージを表示します。
show ipv6 access-list	IPv6 アクセスリストを表示します。
show ipv6 interface	IPv6 インターフェイスのステータスを表示します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

show running-config isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config isakmp** コマンドを使用します。

show running-config isakmp

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
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

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config logging

現在実行されているすべてのロギング コンフィギュレーションを表示するには、特権 EXEC モードで ***show running-config logging*** コマンドを使用します。

show running-config [all] logging [level | disabled]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、ロギング コンフィギュレーションを表示します。
disabled	（オプション）ディセーブルになっているシステム ログ メッセージのコンフィギュレーションのみを表示します。
level	（オプション）デフォルト以外のセキュリティ レベルを持つシステム ログ メッセージのコンフィギュレーションのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 logging** コマンドから変更されました。

例

次に、***show running-config logging disabled*** コマンドの例を示します。

```
hostname# show running-config logging disabled

no logging message 720067
```

関連コマンド

コマンド	説明
logging message	ロギングを設定します。
show logging	ログ バッファおよびその他のロギング設定を表示します。

show logging rate-limit

禁止されたメッセージを元の設定で表示するには、**show logging rate-limit** コマンドを使用します。

show logging rate-limit

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。

コマンドのモード

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	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

情報がクリアされると、ホストが接続を再び確立するまで、何も表示されません。

例

次の例は、禁止されたメッセージを表示する方法を示しています。

```
hostname(config)# show logging rate-limit
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。

show running-config mac-address-table

実行コンフィギュレーションの **mac-address-table static** および **mac-address-table aging-time** のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-address-table** コマンドを使用します。

show running-config mac-address-table

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。

コマンドのモード

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 running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-address-table
mac-address-table aging-time 50
mac-address-table static inside1 0010.7cbe.6101
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show running-config mac-learn

実行コンフィギュレーションの **mac-learn** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-learn** コマンドを使用します。

show running-config mac-learn

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。

コマンドのモード

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 running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-learn
mac-learn disable
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show running-config mac-list

以前に **mac-list** コマンドで指定した MAC アドレスのリストを MAC リスト番号で指定して表示するには、特権 EXEC モードで **show running-config mac-list** コマンドを使用します。

show running-config mac-list *id*

シンタックスの説明

id	16 進形式の MAC アドレス リスト番号です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

show running-config aaa コマンドは、AAA コンフィギュレーションの一部として **mac-list** コマンド文を表示します。

例

次の例は、*id* が adc と等しい MAC アドレス リストを表示する方法を示しています。

```
hostname(config)# show running-config mac-list adc
mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
clear configure mac-list	指定した **mac-list** コマンド文を削除します。
show running-config aaa	実行されている AAA コンフィギュレーションの値を表示します。

show running-config management-access

管理アクセス用に設定されている内部インターフェイスの名前を表示するには、特権 EXEC モードで ***show running-config management-access*** コマンドを使用します。

show running-config management-access

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。

コマンドのモード

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。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は、**nameif** コマンドで定義します。**show interface** コマンドの出力では、二重引用符（"）で囲まれて表示されます）。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname# management-access inside
hostname# show running-config management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show running-config mgcp-map

設定済みの MGCP マップを表示するには、特権 EXEC モードで **show running-config mgcp-map** コマンドを使用します。

show running-config mgcp-map *map_name*

シンタックスの説明.

map_name	指定した MGCP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config mgcp-map コマンドは、設定済みの MGCP マップを表示します。

例

次に、**show running-config mgcp-map** コマンドの出力例を示します。

```
hostname# show running-config mgcp-map mgcp-policy
!
mgcp-map mgcp-policy
call-agent 10.10.11.5 101
call-agent 10.10.11.6 101
call-agent 10.10.11.7 102
call-agent 10.10.11.8 102
gateway 10.10.10.115 101
gateway 10.10.10.116 102
gateway 10.10.10.117 102
command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP デバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
show mgcp	セキュリティ アプライアンスを介して確立された MGCP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show running-config mroute

実行コンフィギュレーションに含まれているスタティック マルチキャスト ルート テーブルを表示するには、特権 EXEC モードで **show running-config mroute** コマンドを使用します。

show running-config mroute [*dst* [*src*]]

シンタックスの説明

dst	マルチキャスト グループの Class D アドレス。
src	マルチキャスト送信元の IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config mroute** コマンドの出力例を示します。

```
hostname# show running-config mroute
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。

show running-config mtu

最大伝送ユニット（maximum transmission unit; MTU）の現在のブロック サイズを表示するには、特権 EXEC モードで **show running-config mtu** コマンドを使用します。

show running-config mtu [*interface_name*]

シンタックスの説明

interface_name	（オプション）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config mtu** コマンドの出力例を示します。

```
hostname# show running-config mtu
mtu outside 1500
mtu inside 1500
mtu dmz 1500
hostname# show running-config mtu outside
mtu outside 1500
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送ユニット（maximum transmission unit; MTU）値を消去します。
mtu	インターフェイスの最大伝送ユニットを指定します。

show running-config multicast-routing

実行コンフィギュレーションに **multicast-routing** コマンドが含まれている場合に、それらのコマンドを表示するには、特権 EXEC モードで **show running-config multicast-routing** コマンドを使用します。

show running-config ***multicast-routing***

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。

コマンドのモード

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

show running-config multicast-routing コマンドは、実行コンフィギュレーションに含まれている **multicast-routing** コマンドを表示します。**multicast-routing** コマンドを実行コンフィギュレーションから削除するには、**clear configure multicast-routing** コマンドを入力します。

例

次に、**show running-config multicast-routing** コマンドの出力例を示します。

```
hostname# show running-config multicast-routing

multicast-routing
```

関連コマンド

コマンド	説明
clear configure multicast-routing	**multicast-routing** コマンドを実行コンフィギュレーションから削除します。
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show running-config name

IP アドレスに関連付けられている（**name** コマンドで設定した）名前のリストを表示するには、特権 EXEC モードで **show running-config name** コマンドを使用します。

show running-config name

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。

コマンドのモード

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)	***running-config*** キーワードが追加されました。

例

次の例は、IP アドレスに関連付けられている名前のリストを表示する方法を示しています。

```
hostname# show running-config name
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。

show running-config nameif

実行コンフィギュレーションのインターフェイス名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config nameif** コマンドを使用します。

show running-config nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

シンタックスの説明

mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスのインターフェイス名コンフィギュレーションが表示されます。

コマンドのモード

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 nameif** から変更されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内でのみ指定できます。

このコマンドの表示内容では、**security-level** コマンドのコンフィギュレーションも示されます。

例

次に、**show running-config nameif** コマンドの出力例を示します。

```
hostname# show running-config nameif
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
!
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイス コンフィギュレーションを消去します。
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。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config names

IP アドレスから名前への変換を表示するには、特権 EXEC モードで **show running-config names** コマンドを使用します。

show running-config names

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。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

names コマンドとともに使用します。

例

次の例は、IP アドレスから名前への変換を表示する方法を示しています。

```
hostname# show running-config names
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。
names	IP アドレスから名前への変換をイネーブルにします。変換の内容は、**name** コマンドで設定できます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。

show running-config nat

ネットワークに関連付けられているグローバル IP アドレスのプールを表示するには、特権 EXEC モードで **show running-config nat** コマンドを使用します。

show running-config nat [*interface_name*] [*nat_id*]

シンタックスの説明

interface_name	（オプション）ネットワーク インターフェイスの名前。
nat_id	（オプション）ホスト グループまたはネットワークの ID。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	キーワード ***running-config*** 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、UDP プロトコルの最大接続値を表示します。UDP 最大接続値が設定されていない場合、この値はデフォルトでは常に 0 と表示され、適用されません。

（注）　透過モードでは、有効となる NAT ID は 0 のみです。

例

次の例は、ネットワークに関連付けられているグローバル IP アドレスのプールを表示する方法を示しています。

```
hostname# show running-config nat
nat (inside) 1001 10.7.2.0 255.255.255.224 0 0
nat (inside) 1001 10.7.2.32 255.255.255.224 0 0
nat (inside) 1001 10.7.2.64 255.255.255.224 0 0
nat (inside) 1002 10.7.2.96 255.255.255.224 0 0
nat (inside) 1002 10.7.2.128 255.255.255.224 0 0
nat (inside) 1002 10.7.2.160 255.255.255.224 0 0
nat (inside) 1003 10.7.2.192 255.255.255.224 0 0
nat (inside) 1003 10.7.2.224 255.255.255.224 0 0
```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーションを削除します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show running-config nat-control

NAT コンフィギュレーションの要件を表示するには、特権 EXEC モードで **show running-config nat-control** コマンドを使用します。

show running-config nat-control

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。

コマンドのモード

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 running-config nat-control** コマンドの出力例を示します。

```
hostname# show running-config nat-control
no nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
nat-control	NAT 規則を設定していない場合でも、内部ホストが外部ネットワークと通信することを許可します。

show running-config ntp

実行コンフィギュレーションの NTP コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ntp** コマンドを使用します。

show running-config ntp

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。

コマンドのモード

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 running-config ntp** コマンドの出力例を示します。

```
hostname# show running-config ntp
ntp authentication-key 1 md5 test2
ntp authentication-key 2 md5 test
ntp trusted-key 1
ntp trusted-key 2
ntp server 10.1.1.1 key 1
ntp server 10.2.1.1 key 2 prefer
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show running-config object-group

現在のオブジェクト グループを表示するには、特権 EXEC モードで **show running-config object-group** コマンドを使用します。

show running-config [**all**] **object-group** [**protocol** | **service** | **network** | **icmp-type** | **id** *obj_grp_id*]

シンタックスの説明

icmp-type	（オプション）ICMP タイプ オブジェクト グループを表示します。
id obj_grp_id	（オプション）指定したオブジェクト グループを表示します。
network	（オプション）ネットワーク オブジェクト グループを表示します。
protocol	（オプション）プロトコル オブジェクト グループを表示します。
service	（オプション）サービス オブジェクト グループを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config object-group** コマンドの出力例を示します。

```
hostname# show running-config object-group
object-group protocol proto_grp_1
    protocol-object udp
    protocol-object tcp
object-group service eng_service tcp
    port-object eq smtp
    port-object eq telnet
object-group icmp-type icmp-allowed
    icmp-object echo
    icmp-object time-exceeded
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。

show running-config passwd

暗号化されたログイン パスワードを表示するには、特権 EXEC モードで **show running-config passwd** コマンドを使用します。

show running-config {**passwd** | **password**}

シンタックスの説明

passwd **|** ***password***	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 passwd** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは ***encrypted*** キーワードとともに表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config passwd** コマンドの出力例を示します。

```
hostname# show running-config passwd
passwd 2AfK9Kjr3BE2/J2r encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。

show running-config pim

実行コンフィギュレーションに含まれている PIM のコマンドを表示するには、特権 EXEC モードで **show running-config pim** コマンドを使用します。

show running-config ***pim***

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。

コマンドのモード

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

show running-config pim コマンドは、グローバル コンフィギュレーション モードで入力された **pim** コマンドを表示します。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドは表示しません。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドを表示するには、**show running-config interface** コマンドを入力します。

例

次に、**show running-config pim** コマンドの出力例を示します。

```
hostname# show running-config pim

pim old-register-checksum
pim spt-threshold infinity
```

関連コマンド

コマンド	説明
clear configure pim	**pim** コマンドを実行コンフィギュレーションから削除します。
show running-config interface	インターフェイス コンフィギュレーション モードで入力されたインターフェイス コンフィギュレーション コマンドを表示します。

show running-config policy-map

すべてまたはデフォルトのポリシーマップ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config policy-map** コマンドを使用します。

show running-config [all] policy-map

シンタックスの説明

all	（オプション）デフォルトのポリシーマップ コンフィギュレーションを表示します。

デフォルト

all キーワードを省略すると、明示的に設定したポリシーマップ コンフィギュレーションのみが表示されます。

コマンドのモード

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

all キーワードを指定すると、明示的に設定したポリシーマップ コンフィギュレーションに加えて、デフォルトのポリシーマップ コンフィギュレーションも表示されます。

例

次の例は、localmap1 というポリシーマップがある場合に、show running-conig policy-map コマンドを使用したときのコマンド出力を示しています。

```
hostname# show running-config policy-map
!
policy-map localmap1
    description this is a test.
    class firstclass
    priority
    ids promiscuous fail0close
    set connection random-seq# enable
    class class-default
!
```

関連コマンド

コマンド	説明
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。
clear configure policy-map	ポリシー コンフィギュレーション全体を削除します。

show running-config pop3s

POP3S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config pop3s** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] pop3s

シンタックスの説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

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。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

例

次に、**show running-config pop3s** コマンドの出力例を示します。

```
hostname# show running-config pop3s

pop3s
 server 10.160.102.188
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all pop3s

pop3s
 port 995
 server 10.160.102.188
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
pop3s	POP3S 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config port-forward

転送された TCP ポートを通じて WebVPN ユーザがアクセスできるアプリケーションのセットを表示するには、特権 EXEC モードで **show running-config port-forward** コマンドを使用します。

show running-config [all] port-forward

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。

コマンドのモード

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 running-config port-forward** コマンドの出力例を示します。

```
hostname# show running-config port-forward

port-forward Telnet 3500 10.148.1.5 23
port-forward Telnet 3501 10.148.1.81 23
port-forward Telnet 3502 10.148.1.82 23
port-forward SSH2 4976 10.148.1.81 22
port-forward SSH2 4977 10.148.1.85 22
port-forward Apps1 10143 flask.CompanyA.com 143
port-forward Apps1 10110 flask.CompanyA.com 110
port-forward Apps1 10025 flask.CompanyA.com 25
port-forward Apps1 11533 sametime-im.CompanyA.com 1533
port-forward Apps1 10022 ddts.CompanyA.com 22
port-forward Apps1 54000 10.148.1.5 23
port-forward Apps1 58000 vpn3060-1 23
port-forward Apps1 58001 vpn3005-1 23
hostname#
```

関連コマンド

コマンド	説明
clear configure port-forward	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
port-forward	WebVPN ユーザがアクセスできるアプリケーションのセットを設定します。
port-forward（webvpn）	ユーザまたはグループポリシーの WebVPN アプリケーション アクセスをイネーブルにします。

show running-config prefix-list

実行コンフィギュレーションに含まれている **prefix-list** コマンドを表示するには、特権 EXEC モードで **show running-config prefix-list** コマンドを使用します。

show running-config prefix-list

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。

コマンドのモード

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 prefix-list** コマンドから **show running-config prefix-list** コマンドに変更されました。

使用上のガイドライン

実行コンフィギュレーションに含まれている **prefix-list description** コマンドは、常に関連する **prefix-list** コマンドの前に表示されます。コマンドを入力した順序は関係しません。

例

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

```
hostname# show running-config prefix-list

!
prefix-list abc description A sample prefix list
prefix-list abc seq 5 permit 192.168.0.0/8 le 24
prefix-list abc seq 10 deny 10.0.0.0/8 le 32
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから消去します。

show running-config priority-queue

インターフェイスのプライオリティキュー コンフィギュレーションの詳細を表示するには、特権 EXEC モードで **show running-config priority-queue** コマンドを使用します。

show running-config priority-queue *interface-name*

シンタックスの説明

interface-name	プライオリティキューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

次の例は、test というインターフェイスについて show running-config priority-queue コマンドを使用した場合のコマンド出力を示しています。

```
hostname# show running-config priority-queue test
priority-queue test
  queue-limit   50
  tx-ring-limit 10
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスからプライオリティキュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイス上に設定されているプライオリティキューの統計情報を表示します。

show running-config privilege

コマンドまたはコマンド セットの特権を表示するには、特権 EXEC モードで **show running-config privilege** コマンドを使用します。

show running-config [all] privilege [**all** | **command** *command* | **level** *level*]

シンタックスの説明

all	（オプション。最初の引数）デフォルトの特権レベルを表示します。
all	（オプション。2 番目の引数）すべてのコマンドの特権レベルを表示します。
command *command*	（オプション）特定のコマンドの特権レベルを表示します。
level *level*	（オプション）指定したレベルに設定されているコマンドを表示します。有効値は 0 ～ 15 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

show running-config privilege コマンドは、現在の特権レベルを表示するために使用します。

例

```
hostname(config)# show running-config privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
privilege	コマンドの特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

show running-config rip

RIP コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config rip** コマンドを使用します。

show running-config [**all**] **rip** [*interface_name*]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての RIP のコマンドを表示します。
interface_name	（オプション）指定したインターフェイスの RIP のコマンドのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 rip** から **show running-config rip** に変更されました。

例

次の例は、RIP 情報を表示する方法を示しています。

```
hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドを消去します。
debug rip	RIP に関するデバッグ情報を表示します。
rip	指定したインターフェイスに RIP を設定します。

show running-config route

セキュリティ アプライアンス上で実行されているルート コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config route** コマンドを使用します。

show running-config [***all***] **route**

シンタックスの説明

デフォルトの動作や値はありません。

デフォルト

このコマンドには、引数もキーワードもありません。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config route** コマンドの出力例を示します。

```
hostname# show running-config route
route outside 10.30.10.0 255.255.255.0 1
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。

show running-config route-map

ルートマップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config route-map** コマンドを使用します。

show running-config route-map [*map_tag*]

シンタックスの説明

map_tag	（オプション）ルートマップ タグのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

show running-config route-map コマンドは、コンフィギュレーション内に定義されているすべてのルートマップを表示するために使用します。名前を指定して個々のルートマップを表示するには、**show running-config route-map** *map_tag* コマンドを使用します。*map_tag* は、ルートマップの名前です。複数のルートマップで同じマップ タグ名を共有できます。

例

次に、**show running-config route-map** コマンドの出力例を示します。

```
hostname# show running-config route-map
route-map maptag1 permit sequence 10
    set metric 5
    match metric 3
route-map maptag1 permit sequence 12
    set metric 5
    match interface backup
    match metric 3
route-map maptag2 deny sequence 10
    match interface dmz
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
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。

show running-config router

ルータ コンフィギュレーションに含まれているグローバル コマンドを表示するには、特権 EXEC モードで **show running-config router** コマンドを使用します。

show running-config [all] **router** [**ospf** [*process_id*]]

シンタックスの説明

all	デフォルトから変更していないコマンドを含めて、すべての router コマンドを表示します。
ospf	（オプション）コンフィギュレーションに含まれている OSPF のコマンドのみを表示します。
process_id	（オプション）選択した OSPF プロセスに関するコマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 router** コマンドから **show running-config router** コマンドに変更されました。

例

次に、**show running-config router** コマンドの出力例を示します。

```
hostname# show running-config router ospf 1
router ospf 1
  log-adj-changes detail
  ignore lsa mospf
  no compatible rfc1583
  distance ospf external 200
  timers spf 10 20
  timers lsa-group-pacing 60
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての router コマンドを消去します。

show running-config same-security-traffic

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表示するには、特権 EXEC モードで **show running-config same-security-traffic** コマンドを使用します。

show running-config same-security-traffic

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。

コマンドのモード

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 running-config same-security-traffic** コマンドの出力例を示します。

```
hostname# show running-config same-security-traffic
```

関連コマンド

コマンド	説明
same-security-traffic	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許可します。

show running-config service

システム サービスを表示するには、特権 EXEC モードで **show running-config service** コマンドを使用します。

show running-config service

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。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次のコマンドは、システム サービスを表示する方法を示しています。

```
hostname# show running-config service
service resetoutside
```

関連コマンド

コマンド	説明
service	システム サービスをイネーブルにします。

show running-config service-policy

現在実行されているすべてのサービス ポリシー コンフィギュレーションを表示するには、グローバル コンフィギュレーション モードで ***show running-config service-policy*** コマンドを使用します。

show running-config service-policy

シンタックスの説明

default	デフォルトのサービス ポリシーを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	このコマンドが導入されました。

例

次に、***show running-config service-policy*** コマンドの例を示します。

```
hostname# show running-config service-policy
```

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。
service-policy	サービス ポリシーを設定します。
clear 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。
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。

show running-configuration smtps

SMTPS の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-configuration smtps** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-configuration [all] smtps

シンタックスの説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

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。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

例

次に、**show running-config smtps** コマンドの出力例を示します。

```
hostname# show running-configuration smtps

smtps
server 10.1.1.21
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all smtps

smtps
 port 995
 server 10.1.1.21
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
hostname#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
smtps	SMTPS 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config snmp-map

設定済みの SNMP マップを表示するには、特権 EXEC モードで **show running-config snmp-map** コマンドを使用します。

show running-config snmp-map *map_name*

シンタックスの説明.

map_name	指定した SNMP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

show running-config snmp-map コマンドは、設定済みの SNMP マップを表示します。

例

次に、**show running-config snmp-map** コマンドの出力例を示します。

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

show running-config snmp-server

現在実行されているすべての SNMP サーバのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モードで ***show running-config snmp-server*** コマンドを使用します。

show running-config [default] snmp-server

シンタックスの説明

default	デフォルト SNMP サーバのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
PIX Version 7.0	このコマンドが導入されました。

例

次に、***show running-config snmp-server*** コマンドの例を示します。

```
hostname# show running-config snmp-server
```

関連コマンド

コマンド	説明
snmp-server	SNMP サーバを設定します。
clear snmp-server	SNMP サーバのコンフィギュレーションを消去します。
show snmp-server statistics	SNMP サーバのコンフィギュレーションを表示します。

show running-config ssh

現在のコンフィギュレーションに含まれている SSH のコマンドを表示するには、特権 EXEC モードで **show running-config ssh** コマンドを使用します。

show running-config [***default***] ***ssh*** [***timeout*** | ***version***]

show run [***default***] ***ssh*** [***timeout***]

シンタックスの説明

default	（オプション）設定済みの SSH コンフィギュレーション値に加えて、デフォルトの値も表示します。
timeout	（オプション）現在の SSH セッション タイムアウト値を表示します。
version	（オプション）現在サポートされている SSH のバージョンを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 ssh** コマンドから **show running-config ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、現在の SSH コンフィギュレーションを表示します。SSH セッション タイムアウト値のみを表示するには、***timeout*** オプションを使用します。アクティブな SSH セッションのリストを表示するには、**show ssh sessions** コマンドを使用します。

例

次の例では、SSH セッション タイムアウトを表示しています。

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

show running-config ssl

現在の一連の設定済み ssl コマンドを表示するには、特権 EXEC モードで **show running-config ssl** コマンドを使用します。

show running-config ssl

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	•	•	•	•
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、show running-config ssl コマンドの出力例を示します。

```
hostname# show running-config ssl
ssl server-version  tlsv1
ssl client-version tlsv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

show running-config static

コンフィギュレーションに含まれているすべての **static** コマンドを表示するには、特権 EXEC モードで **show running-config static** コマンドを使用します。

show running-config static

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。

コマンドのモード

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)	キーワード ***running-config*** 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、UDP プロトコルの最大接続値を表示します。UDP 最大接続値が「0」または設定されていない場合、制限の実施はディセーブルになります。

例

次の例は、コンフィギュレーションに含まれているすべての static コマンドを表示する方法を示しています。

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```

（注） UDP 接続の制限値は表示されません。

関連コマンド

コマンド	説明
clear configure static	すべての **static** コマンドをコンフィギュレーションから削除します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

show running-config sunrpc-server

SunRPC コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config sunrpc-server** コマンドを使用します。

show running-config sunrpc-server *interface_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

シンタックスの説明

interface_name	サーバのインターフェイス。
ip_addr	サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* **-** *port*	SunRPC プロトコルのポート範囲。または、2 番目のポートを指定します。
protocol	SunRPC 転送プロトコル。
service	サービスを指定します。
service_type	SunRPC サービス プログラム タイプを設定します。
timeout *hh:mm:ss*	タイムアウト アイドル期間を指定します。この期間を過ぎると、SunRPC サービス トラフィックへのアクセスが終了します。
TCP	（オプション）TCP を指定します。
UDP	（オプション）UDP 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。

コマンドのモード

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

service_type は、**sunrpcinfo** コマンドで指定したものです。

例

次に、**show running-config sunrpc-server** コマンドの出力例を示します。

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout
0:03:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	SunRPC サービスをセキュリティ アプライアンスから消去します。
debug sunrpc	SunRPC のデバッグ情報をイネーブルにします。
show conn	SunRPC など、さまざまな接続タイプの接続状態を表示します。
sunrpc-server	SunRPC サービス テーブルを作成します。
timeout	SunRPC を含む、さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show running-config sysopt

実行コンフィギュレーションの **sysopt** コマンド コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config sysopt** コマンドを使用します。

show running-config sysopt

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。

コマンドのモード

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 sysopt** コマンドから変更されました。

例

次に、**show running-config sysopt** コマンドの出力例を示します。

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

show running-config tcp-map

TCP マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config tcp-map** コマンドを使用します。

show running-config tcp-map [*tcp_map_name*]

シンタックスの説明

tcp_map_name	（オプション）TCP マップ名のテキスト。テキストの長さは、58 文字までです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 running-config tcp-map** コマンドの出力例を示します。

```
hostname# show running-config tcp-map
tcp-map localmap
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。
clear configure tcp-map	TCP マップのコンフィギュレーションを消去します。

show running-config telnet

セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示するには、特権 EXEC モードで **show running-config telnet** コマンドを使用します。また、このコマンドを使用して、Telnet セッションに許容されるアイドル時間（分）を表示することもできます。このアイドル時間が経過すると、その Telnet セッションはセキュリティ アプライアンスが終了します。

show running-config telnet [**timeout**]

シンタックスの説明

timeout	（オプション）Telnet セッションに許容されるアイドル時間（分）で、アイドル時間が経過すると、その Telnet セッションはセキュリティ アプライアンスが終了します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	キーワード ***running-config*** が追加されました。

例

次の例は、セキュリティ アプライアンスへの Telnet 接続で使用することを認可されている IP アドレスの現在のリストを表示する方法を示しています。

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

show running-config terminal

現在の端末設定を表示するには、特権 EXEC モードで ***show running-config terminal*** コマンドを使用します。

show running-config terminal

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンドのモード

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)	***running-config*** キーワードが追加されました。

例

次の例では、ページの長さの設定がクリアされます。

```
hostname# show running-config terminal

Width = 80, no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。

show running-config tftp-server

デフォルト TFTP サーバのアドレスとディレクトリを表示するには、グローバル コンフィギュレーション モードで **show running-config tftp-server** コマンドを使用します。

show running-config tftp-server

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。

コマンドのモード

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)	***running-config*** キーワードが追加されました。

例

次の例は、デフォルト TFTP サーバの IP/IPv6 アドレスとコンフィギュレーション ファイルのディレクトリを表示する方法を示しています。

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

関連コマンド

コマンド	説明
configure net	コンフィギュレーションを TFTP サーバ上の指定パスからロードします。
tftp-server	デフォルト TFTP サーバのアドレスとコンフィギュレーション ファイルのディレクトリを設定します。

show running-config timeout

すべてまたは特定のプロトコルのタイムアウト値を表示するには、特権 EXEC モードで **show running-config timeout** コマンドを使用します。

show running-config timeout *protocol*

シンタックスの説明

protocol	（オプション）指定したプロトコルのタイムアウト値を表示します。サポートされているプロトコルは、**xlate**、**conn**、**udp**、**icmp**、**rpc**、**h323**、**h225**、**mgcp**、***mgcp-pat***、**sip**、**sip_media**、および **uauth** です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	***running-config*** キーワードと ***mgcp-pat*** キーワードが追加されました。

例

次の例は、システムのタイムアウト値を表示する方法を示しています。

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

関連コマンド

コマンド	説明
clear configure timeout	デフォルトのアイドル期間に戻します。
timeout	アイドル状態の最大継続時間を設定します。

show running-config tunnel-group

すべてまたは特定のトンネルグループおよびトンネルグループ アトリビュートについて、コンフィギュレーション情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config tunnel-group** コマンドを使用します。

show running-config [**all**] ***tunnel-group*** [*name* [**general-attributes | ipsec-attributes | ppp-attributes**]]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての tunnel-group コマンドを表示します。
general-attributes	一般アトリビュートのコンフィギュレーション情報を表示します。
ipsec-attributes	IPSec アトリビュートのコンフィギュレーション情報を表示します。
name	トンネルグループの名前を指定します。
ppp-attributes	PPP アトリビュートのコンフィギュレーション情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•		•		
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

グローバル コンフィギュレーション モードで入力した次の例では、すべてのトンネルグループの現在のコンフィギュレーションを表示しています。

```
hostname<config># show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname<config>#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネルグループのコンフィギュレーションを削除します。
tunnel-group general-attributes	指定したトンネルグループの一般アトリビュートを指定するための、サブコンフィギュレーション モードに入ります。
tunnel-group ipsec-attributes	指定したトンネルグループの IPSec アトリビュートを指定するための、サブコンフィギュレーション モードに入ります。
tunnel-group	指定したタイプのトンネルグループ サブコンフィギュレーション モードに入ります。

show running-config url-block

URL フィルタリングで使用されるバッファとメモリ割り当てのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-block** コマンドを使用します。

show running-config url-block [**block** | **url-mempool** | **url-size**]

シンタックスの説明

block	バッファされるブロックの最大数に関するコンフィギュレーションを表示します。
url-mempool	許容される最大の URL サイズ（KB 単位）に関するコンフィギュレーションを表示します。
url-size	長い URL のバッファに割り当てられるメモリ リソース（KB 単位）に関するコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config url-block コマンドは、URL フィルタリングで使用されるバッファとメモリ割り当てのコンフィギュレーションを表示します。

例

次に、**show running-config url-block** コマンドの出力例を示します。

```
hostname# show running-config url-block
!
url-block block 56
!
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタをクリアします。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config url-cache

URL フィルタリングで使用されるキャッシュのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-cache** コマンドを使用します。

show running-config url-cache

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config url-cache コマンドは、URL フィルタリングで使用されるキャッシュのコンフィギュレーションを表示します。

例

次に、**show running-config url-cache** コマンドの出力例を示します。

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-configuration url-list

WebVPN ユーザがアクセスできる URL のセットを表示するには、特権 EXEC モードで **show running-configuration url-list** コマンドを使用します。

show running-configuration url-list

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。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
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

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

```
hostname# show running-configuration url-list
url-list userURL "SW Engineering" http://10.1.1.2
url-list userURL "My Company" http://www.mycompany.com
url-list userURL "401K Program" https://401k.com
url-list userURL "Exchange5.5 Mail" http://10.1.1.11/exchange
url-list URLlist2 "OWA-2000" http://10.1.1.7/exchange
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定します。
url-list	特定のグループポリシーまたはユーザの WebVPN URL アクセスをイネーブルにします。

show running-config url-server

URL フィルタリング サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-server** コマンドを使用します。

show running-config url-server

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show running-config url-server コマンドは、URL フィルタリング サーバのコンフィギュレーションを表示します。

例

次に、**show running-config url-server** コマンドの出力例を示します。

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config username

特定のユーザの実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config username** コマンドをユーザ名を付加して使用します。すべてのユーザの実行コンフィギュレーションを表示するには、ユーザ名を指定せずにこのコマンドを使用します。

show running-config [**all**] **username** [*name*] [**attributes**]]

シンタックスの説明

attributes	ユーザの特定の AVP を表示します。
all	（オプション）デフォルトから変更していないコマンドを含めて、すべてのユーザ名についてコマンドを表示します。
name	ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
ユーザ名	•	—	•	—	—

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、anyuser というユーザについての show running-config username コマンドの出力例を示します。

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースを消去します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	特定のユーザのアトリビュートを設定できます。

show running-config virtual

セキュリティ アプライアンス仮想サーバの IP アドレスを表示するには、特権 EXEC モードで **show running-config virtual** コマンドを使用します。

show running-config [**all**] **virtual**

シンタックスの説明

all	すべての仮想サーバの仮想サーバ IP アドレスを表示します。

デフォルト

all キーワードを省略すると、現在の仮想サーバ（複数の場合あり）に対して明示的に設定した IP アドレスのみが表示されます。

コマンドのモード

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)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドを使用するには、特権 EXEC モードに入っている必要があります。

例

次に、設定済みの HTTP 仮想サーバが存在する場合の **show running-config virtual** コマンドの出力例を示します。

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
virtual	認証仮想サーバのアドレスを表示します。

show running-config vpn load-balancing

現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロードバランシング モードで **show running-config vpn load-balancing** コマンドを使用します。

show running-config [all] vpn load-balancing

シンタックスの説明

all	デフォルトおよび明示的に設定した VPN ロードバランシング コンフィギュレーションを両方とも表示します。

デフォルト

all キーワードを省略すると、明示的に設定した VPN ロードバランシング コンフィギュレーションが表示されます。

コマンドのモード

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	•	—	•	—	—
特権 EXEC	•	—	•	—	—
VPN ロードバランシング	•	—	•	—	—

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

show running-config vpn load-balancing コマンドは、関連コマンドである **cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、および **priority** に関するコンフィギュレーション情報も表示します。

例

次に、***all*** オプションをイネーブルにした **show running-config vpn load-balancing** コマンドとその出力例を示します。

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
 no nat
 priority 9
 interface lbpublic test
 interface lbprivate inside
 no cluster ip address
 no cluster encryption
 cluster port 9023
 no participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド文を削除します。
show vpn load-balancing	VPN ロードバランシングの実行時の統計情報を表示します。
vpn load-balancing	vpn ロードバランシング モードに入ります。

show running-configuration vpn-sessiondb

現在の一連の設定済み vpn-sessiondb コマンドを表示するには、特権 EXEC モードで **show running-configuration vpn-sessiondb** コマンドを使用します。

show running-configuration [all] vpn-sessiondb

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **vpn-sessiondb** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

リリース 7.0 以降では、このコマンドは VPN 最大セッション制限のみを表示します（設定されている場合）。

例

次に、**show running-configuration vpn-sessiondb** コマンドの出力例を示します。

```
hostname# show running-configuration vpn-sessiondb
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show running-configuration webvpn

webvpn の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-configuration webvpn** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-configuration [all] webvpn

シンタックスの説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

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。

コマンドのモード

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	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

例

次に、**show running-config webvpn** コマンドの出力例を示します。

```
hostname# show running-configuration webvpn
webvpn
 title WebVPN Services for ASA-4
 title-color green
 default-idle-timeout 0
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 authorization-dn-attributes CN

hostname#(config-webvpn)# show running-config all webvpn

webvpn
 title WebVPN Services for ASA-4
 username-prompt Username
 password-prompt Password
 login-message Please enter your username and password
 logout-message Goodbye
 no logo
 title-color green
 secondary-color #CCCCFF
 text-color white
 secondary-text-color black
 default-idle-timeout 0
 no http-proxy
 no https-proxy
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 no authorization-server-group
 default-group-policy DfltGrpPolicy
 authentication aaa
 no authorization-required
 authorization-dn-attributes CN
hostname#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
smtps	SMTPS 電子メール プロキシのコンフィギュレーションを作成または編集します。

show service-policy

設定済みのサービス ポリシーを表示するには、グローバル コンフィギュレーション モードで ***show service-policy*** コマンドを使用します。

show service-policy [**global** | ***interface*** *intf*] [***inspect*** | ***ips*** | ***police*** | ***priority*** | ***set connection***]

show service-policy [**global** | ***interface*** *intf*] [***flow*** *protocol* {***host*** *src_host* | *src_ip src_mask*} [***eq*** *src_port*] {***host*** *dest_host* | *dest_ip dest_mask*} [***eq*** *dest_port*] [*icmp_number* | *icmp_control_message*]]

シンタックスの説明

dest_ip	トラフィック フローの宛先 IP アドレス。
dest_mask	トラフィック フローの宛先 IP アドレスのサブネット マスク。
dest_port	（オプション）トラフィック フローで使用されている宛先ポート。
eq	（オプション）等号。送信元または宛先のポートが、以降に指定するポート番号と一致することを要求します。
flow	（オプション）セキュリティ アプライアンスでポリシーの適用対象となるトラフィック フローを指定します。このフローに適用されるポリシーが表示されます。***flow*** キーワードに続いて指定する引数とキーワードでは、フローを IP 5 タプル形式で指定します。
global	（オプション）すべてのインターフェイスに適用されるグローバル ポリシーのみを出力します。
host *dest_host*	トラフィック フローの宛先ホストの IP アドレス。
host *src_host*	トラフィック フローの送信元ホストの IP アドレス。
icmp_control_message	（オプション）トラフィック フローの ICMP 制御メッセージを指定します。*icmp_control_message* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
icmp_number	（オプション）トラフィック フローの ICMP プロトコル番号を指定します。
inspect	（オプション）**inspect** コマンドを含んでいるポリシーのみを出力します。
interface *intf*	（オプション）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* は、**nameif** コマンドで定義したインターフェイス名です。
ips	（オプション）**ips** コマンドを含んでいるポリシーのみを出力します。
police	**police** コマンドを含んでいるポリシーのみを出力します。
priority	**priority** コマンドを含んでいるポリシーのみを出力します。
set connection	**set connection** コマンドを含んでいるポリシーのみを出力します。
protocol	トラフィック フローで使用されているプロトコル。*protocol* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
src_ip	トラフィック フローで使用されている送信元 IP アドレス。
src_mask	トラフィック フローで使用されている送信元 IP ネットマスク。
src_port	トラフィック フローで使用されている送信元ポート。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード　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
7.0(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　***flow*** キーワードを使用すると、記述可能な任意のフローについて、セキュリティ アプライアンスがそのフローに適用するポリシーを特定できます。この情報を利用すると、必要なサービスがこのサービス ポリシー コンフィギュレーションによって特定の接続に提供されるかどうかを確認できます。***flow*** キーワード以降に指定する引数とキーワードでは、オブジェクト グループ化をしていないフローを IP 5 タプル形式で指定します。

フローを IP 5 タプル形式で記述するため、すべての一致基準がサポートされるわけではありません。次に、フローの検索でサポートされている一致基準のリストを示します。

- ***match access-list***
- ***match port***
- ***match rtp***
- ***match default-inspection-traffic***

priority キーワードは、インターフェイスを経由して転送されたパケットの集約カウンタ値を表示するために使用します。

show service-policy コマンドの出力に表示される初期接続の数は、**class-map** コマンドで定義したトラフィック マッチングと一致したインターフェイスに向かう現在の初期接続の数を示しています。`embryonic-conn-max` フィールドは、モジュラ ポリシー フレームワークを使用するトラフィック クラスに対して設定した最大初期接続数の制限値を示しています。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続が **class-map** コマンドで定義したトラフィック タイプと一致すると、その接続に対して TCP 代行受信が適用されます。

protocol 引数の値

次に、*protocol* 引数で有効となる値を示します。

- *number*：プロトコル番号（0 ～ 255）
- ***ah***
- ***eigrp***
- ***esp***
- ***gre***
- ***icmp***
- ***icmp6***
- ***igmp***
- ***igrp***
- ***ip***

- *ipinip*
- *ipsec*
- *nos*
- *ospf*
- *pcp*
- *pim*
- *pptp*
- *snp*
- *tcp*
- *udp*

icmp_control_message 引数の値

次に、*icmp_control_message* 引数で有効となる値を示します。

- *alternate-address*
- *conversion-error*
- *echo*
- *echo-reply*
- *information-reply*
- *information-request*
- *mask-reply*
- *mask-request*
- *mobile-redirect*
- *parameter-problem*
- *redirect*
- *router-advertisement*
- *router-solicitation*
- *source-quench*
- *time-exceeded*
- *timestamp-reply*
- *timestamp-request*
- *traceroute*
- *unreachable*

例

次の例は、***show service-policy*** コマンドのシンタックスを示しています。

```
hostname# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
hostname# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap


hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq
5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。
clear service-policy	すべてのサービス ポリシーのコンフィギュレーションを消去します。
service-policy	サービス ポリシーを設定します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show service-policy inspect gtp

GTP コンフィギュレーションを表示するには、特権 EXEC モードで **show service-policy inspect gtp** コマンドを使用します。

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | ***pdpmcb*** | **requests** | **statistics** [**gsn** *IP_address*] }

シンタックスの説明.

apn	（オプション）指定した APN に基づいて、PDP コンテキストの詳細な出力を表示します。
ap_name	統計情報を表示する特定のアクセス ポイント名を指定します。
detail	（オプション）PDP コンテキストの詳細な出力を表示します。
imsi	指定した IMSI に基づいて、PDP コンテキストの詳細な出力を表示します。
IMSI_value	統計情報を表示する特定の IMSI を指定するための 16 進値。
interface	（オプション）特定のインターフェイスを指定します。
int	情報を表示するインターフェイスを指定します。
gsn	（オプション）GPRS サポート ノードを指定します。このノードは、GPRS 無線データ ネットワークとその他のネットワークの間にあるインターフェイスです。
gtp	（オプション）GTP のサービス ポリシーを表示します。
IP_address	統計情報を表示する IP アドレス。
ms-addr	（オプション）指定したモバイル ステーション（MS）アドレスに基づいて、PDP コンテキストの詳細な出力を表示します。
pdp-context	（オプション）パケット データ プロトコル コンテキストを指定します。
pdpmcb	（オプション）PDP マスター制御ブロックのステータスを表示します。
requests	（オプション）GTP 要求のステータスを表示します。
statistics	（オプション）GTP 統計情報を表示します。
tid	（オプション）指定した TID に基づいて、PDP コンテキストの詳細な出力を表示します。
tunnel_ID	統計情報を表示する特定のトンネルを指定するための 16 進値。
version	（オプション）GTP バージョンに基づいて、PDP コンテキストの詳細な出力を表示します。
version_num	統計情報を表示する PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

縦線（|）を使用すると、表示内容をフィルタリングできます。表示フィルタリング オプションの詳細については、| を入力してください。

show pdp-context コマンドは、PDP コンテキストに関する情報を表示します。

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合せであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション ユーザの間で転送するために必要なものです。

show gtp requests コマンドは、要求キューに入っている現在の要求を表示します。

例

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

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦線（|）を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次のコマンドでは、GTP 検査の統計情報を表示しています。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次のコマンドでは、PDP コンテキストに関する情報を表示しています。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 7-27 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各カラムの説明を示します。

表 7-27　PDP コンテキスト

カラムのヘッダー	説明
Version	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr	サービス提供ゲートウェイ サービス ノードを表示します。
Idle	PDP コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に特定の GTP マップを適用します。

show shun

排除情報を表示するには、特権 EXEC モードで **show shun** コマンドを使用します。

show shun [*src_ip* | *statistics*]

シンタックスの説明

src_ip	（オプション）このアドレスに関する情報を表示します。
statistics	（オプション）インターフェイスのカウンタのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 shun** コマンドの出力例を示します。

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
shun	新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにします。

show sip

SIP セッションを表示するには、特権 EXEC モードで **show sip** コマンドを使用します。

show sip

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。

コマンドのモード

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。

使用上のガイドライン

show sip コマンドは、SIP 検査エンジンの問題のトラブルシューティングに役立ちます。説明は、**inspect protocol sip udp 5060** コマンドと一緒にします。**show timeout sip** コマンドは、指示されているプロトコルのタイムアウト値を表示します。

show sip コマンドは、セキュリティ アプライアンスを越えて確立されている SIP セッションの情報を表示します。**debug sip** と **show local-host** コマンドと共に、このコマンドは、SIP 検査エンジンの問題のトラブルシューティングに使用されます。

（注）　**show sip** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの SIP セッション レコードが存在し、**pager** コマンドが設定されていない場合、**show sip** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 state Active, idle 0:00:06
```

この例は、セキュリティ アプライアンス上の 2 つのアクティブな SIP セッションを示しています（Total フィールドで示されているように）。各 call-id は、コールを表わしています。

最初のセッションは、call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションはまだコール セットアップ中であることを示しています。コール セットアップが完了するのは、ACK が確認されたときのみです。このセッションは、1 秒間アイドル状態でした。

2 番目のセッションは、Active 状態です。ここでは、コール セットアップは完了して、エンドポイントはメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug sip	SIP のデバッグ情報をイネーブルにします。
inspect sip	SIP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show skinny

SCCP（Skinny）検査エンジンの問題をトラブルシューティングするには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny

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。

コマンドのモード

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。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）検査エンジンの問題のトラブルシューティングに役立ちます。

例

次の条件での **show skinny** コマンドの出力例を示します。セキュリティ アプライアンスを越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
hostname# show skinny

        LOCAL                   FOREIGN                 STATE

----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力は、両方の内部 Cisco IP Phone 間でコールが確立されていることを示します。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show snmp-server statistics

SNMP 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 snmp-server statistics** コマンドを使用します。

show snmp-server 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

このコマンドにデフォルト設定はありません。

コマンドのモード

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

この例は、SNMP サーバ統計情報を表示する方法を示しています。

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
clear configure snmp-server	簡易ネットワーク管理プロトコル(SNMP)サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバのコンフィギュレーションを表示します。

show ssh sessions

セキュリティ アプライアンス上のアクティブな SSH セッションの情報を表示するには、特権 EXEC モードで **show ssh sessions** コマンドを使用します。

show ssh *sessions* [*ip_address*]

シンタックスの説明

ip_address	（オプション）指定した IP アドレスのセッション情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

SID は、SSH セッションを識別する一意な番号です。Client IP は、SSH クライアントを実行しているシステムの IP アドレスです。Version は、SSH クライアントがサポートしているプロトコル バージョン番号です。SSH が SSH バージョン 1 のみサポートしている場合、Version カラムには 1.5 が表示されます。SSH クライアントが SSH バージョン 1 と SSH バージョン 2 の両方をサポートしている場合、Version カラムには 1.99 が表示されます。SSH クライアントが SSH バージョン 2 のみサポートしている場合、Version カラムには 2.0 が表示されます。Encryption カラムには、SSH クライアントが使用している暗号化のタイプが表示されます。State カラムには、クライアントとセキュリティ アプライアンスとの対話の進捗状況が表示されます。Username カラムには、セッションで認証されているログイン ユーザ名が表示されます。

例

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

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

関連コマンド

コマンド	説明
ssh disconnect	アクティブな SSH セッションを切断します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

show startup-config

スタートアップ コンフィギュレーションを表示するには、特権 EXEC モードで show startup-config コマンドを使用します。

show startup-config

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。

コマンドのモード

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。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドは現在の実行スペース（システム コンフィギュレーションまたはセキュリティ コンテキスト）のスタートアップ コンフィギュレーションを表示します。

例

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

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.0(0)28
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

関連コマンド

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

show sunrpc-server active

Sun RPC サービス用に開いているピンホールを表示するには、特権 EXEC モードで **show sunrpc-server active** コマンドを使用します。

show sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show sunrpc-server active コマンドは、NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するために使用します。

例

Sun RPC サービス用に開いているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールを消去します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	Sun RPC サービスのコンフィギュレーションに関する情報を表示します。

show tcpstat

セキュリティ アプライアンスの TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを（デバッグのために）表示するには、特権 EXEC モードで **show tcpstat** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show tcpstat

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。

コマンドのモード

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。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを表示できます。表 7-28 は、表示される TCP 統計情報を説明しています。

表 7-28　show tcpstat コマンドでの TCP 統計情報

統計情報	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可によって使用されます。
tcp_xmt pkts	TCP スタックによって送信されたパケットの数。
tcp_rcv good pkts	TCP スタックによって受信された正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	不良チェックサムを保持していた受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザを追加しようとしたときに、ユーザがすでにハッシュ テーブル内に存在していた回数。
tcp user srch hash hit	検索時に TCP ユーザがハッシュ テーブル内で検出された回数。
tcp user srch hash miss	検索時に TCP ユーザがハッシュ テーブル内で検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたときに、ユーザがハッシュ テーブル内で検出されなかった回数。

表 7-28　show tcpstat コマンドでの TCP 統計情報（続き）

統計情報	説明
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態（RFC 793 を参照）。表示される値を次に示します。 1　CLOSED 2　LISTEN 3　SYN_SENT 4　SYN_RCVD 5　ESTABLISHED 6　FIN_WAIT_1 7　FIN_WAIT_2 8　CLOSE_WAIT 9　CLOSING 10　LAST_ACK 11　TIME_WAIT
rexqlen	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値（ミリ秒）。
to_timer	TCP ユーザの非活動タイムアウト タイマーの値（ミリ秒）。
cl_timer	TCP ユーザのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザの持続タイマーの値（ミリ秒）。
rt_timer	TCP ユーザの再送信タイマーの値（ミリ秒）。
tries	TCP ユーザの再送信カウント。

例

次の例は、セキュリティ アプライアンスの TCP スタックのステータスを表示する方法を示しています。

```
hostname# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [**detail** | **file** | **no-config**]

シンタックスの説明

detail	（オプション）詳細情報を表示します。
file	（オプション）コマンドの出力をファイルに書き込みます。
no-config	（オプション）実行コンフィギュレーションの出力を除外します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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)	***detail*** キーワードと ***file*** キーワードが追加されました。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。**show** コマンドからの出力を組み合せて、テクニカル サポート アナリストに対して最も多くの情報を提供します。

例

次の例は、テクニカル サポートで分析に使用する情報を、実行コンフィギュレーションの出力を除外して表示する方法を示しています。

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
```

```
Guards:              Enabled
URL-filtering:       Enabled
Inside Hosts:        Unlimited
Throughput:          Unlimited
IKE peers:           Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Apr 17 2005

------------------ show memory ------------------

Free memory:         50708168 bytes
Used memory:         16400696 bytes
-------------      ----------------
Total memory:        67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
```

```
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


     PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8           0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8           0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18           0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718           0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8           0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8           0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8           0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8           0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8           0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8           0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8           0 00d3a354 3780/4096 XXX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8           0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8           0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90           0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8           0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920           0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8           0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30           0 00e7ad1c 3704/4096 XXX/trace
Lwe 002e471e 00e7cc44 00553368           0 00e7bdcc 3704/4096 XXX/tconsole
Hwe 001e5368 00e7ed44 00730674           0 00e7ce9c 7228/8192 XXX/intf0
Hwe 001e5368 00e80e14 007305d4           0 00e7ef6c 7228/8192 XXX/intf1
Hwe 001e5368 00e82ee4 00730534        2470 00e8103c 4892/8192 XXX/intf2
H*  0011d7f7 0009ff2c 0053e5b0         780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8           0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360           0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0           0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20           0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8           0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40   121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8           0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0           0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48          20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc           0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198           0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174           0 00f475a4 3832/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150           0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850           0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c           0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108           0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4           0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0           0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534           0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c           0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078           0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054           0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8           0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8           0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------
```

```
No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

関連コマンド

コマンド	説明
show clock	Syslog Server（PFSS）と公開キー インフラストラクチャ（PKI）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータス、およびどのセキュリティ アプライアンスがアクティブになっているかを表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	セキュリティ アプライアンスのパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	セキュリティ アプライアンス上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show traffic

インターフェイスの送信アクティビティと受信アクティビティを表示するには、特権 EXEC モードで ***show traffic*** コマンドを使用します。

show traffic

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。

コマンドのモード

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。

使用上のガイドライン

show traffic コマンドは、show traffic コマンドが最後に入力された時点またはセキュリティ アプライアンスがオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、セキュリティ アプライアンスが直近のリブート以降、オンラインになってからの経過時間です（直近のリブート以降に **clear traffic** コマンドが入力されていない場合）。このコマンドが入力されていた場合、この秒数は、コマンドが入力された時点からの経過時間です。

例

次に、**show traffic** コマンドの出力例を示します。

```
hostname# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

関連コマンド

コマンド	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。

show uauth

現在認証されている 1 人またはすべてのユーザ、ユーザがバインドされているホスト IP、キャッシュされた IP およびポート認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

show uauth [*username*]

シンタックスの説明

username	（オプション）表示するユーザ認証情報とユーザ認可情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認可情報が表示されます。

コマンドのモード

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。

使用上のガイドライン

show uauth コマンドは、1 人またはすべてのユーザの AAA 認可キャッシュと AAA 認証キャッシュを表示します。

timeout コマンドと共に使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。ユーザ ホストごとにアドレスとサービスのペアを最大 16 個までキャッシュできます。ユーザが適切なホストから、キャッシュされたサービスにアクセスしようとすると、セキュリティ アプライアンスはユーザを認可済みであると見なし、すぐに接続を代理処理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、各イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。このプロセスにより、認可サーバ上でパフォーマンスが大幅に向上し、負荷も大幅に軽減されます。

show uauth コマンドの出力では、認証および認可の目的で認可サーバに提供されたユーザ名が表示されます。また、ユーザ名がバインドされている IP アドレス、ユーザが認証されただけであるか、キャッシュされたサービスを持っているかが表示されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、Xauth を Easy VPN Remote 機能とともにネットワーク拡張モードで使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドの項を参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザが認証されておらず、1 人のユーザの認証が進行中である場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

次に、3 人のユーザが認証され、セキュリティ アプライアンスを介してサービスを使用することを認可されている場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

関連コマンド

コマンド	説明
clear uauth	現在のユーザの認証情報と認可情報を削除します。
timeout	アイドル状態の最大継続時間を設定します。

show url-block

url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（あれば）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

show url-block [**block statistics**]

シンタックスの説明

block statistics	（オプション）ブロック バッファ使用状況の統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show url-block block statistics コマンドは、url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（あれば）を表示します。

例

次に、**show url-block** コマンドの出力例を示します。

```
hostname# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

URL ブロック バッファのコンフィギュレーションが表示されています。

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

```
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-cache statistics

N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される、URL キャッシュに関する情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

show url-cache 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。

コマンドのモード　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。

使用上のガイドライン　**show url-cache statistics** コマンドは、次のエントリを表示します。

- Size：KB 単位で表したキャッシュ サイズ。**url-cache** *size* オプションを使用して設定します。
- Entries：キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use：現在キャッシュにあるエントリ数。
- Lookups：セキュリティ アプライアンスがキャッシュ エントリを検索した回数。
- Hits：セキュリティ アプライアンスがキャッシュ内でエントリを検出した回数。

show perfmon コマンドを使用して、N2H2 Sentian または Websense フィルタリング アクティビティに関する追加情報を表示できます。

例

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

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :      1KB
 Entries :      36
  In Use :      30
 Lookups :      300
 Hits :      290
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-server

URL フィルタリング サーバに関する情報を表示するには、特権 EXEC モードで **show url-server** コマンドを使用します。

show url-server 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。

コマンドのモード

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。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバ ベンダー、URL の合計数、許可された数、拒否された数、HTTPS 接続の合計数、許可された数、拒否された数、TCP 接続の合計数、許可された数、拒否された数、および URL サーバ ステータスを表示します。

show url-server コマンドは、次の情報を表示します。

- N2H2 の場合 : **url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- Websense の場合 : **url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

例

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

```
hostname## show url-server statistics

URL Server Statistics:
Vendor websense
HTTPs total/allowed/denied 0/0/0
HTTPSs total/allowed/denied 0/0/0
FTPs total/allowed/denied 0/0/0
URL Server Status:
172.23.58.103 UP
URL Packets Send and Receive Stats:
Message Send Receive
STATUS_REQUEST 200 200
LOOKUP_REQUEST 10 10
LOG_REQUEST 20 NA
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show version

ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示するには、特権 EXEC モードで **show version** コマンドを使用します。

show version

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。

コマンドのモード　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
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show version** コマンドを使用すると、ソフトウェア バージョン、最後にリブートされて以降の動作時間、プロセッサ タイプ、フラッシュ パーティション タイプ、インターフェイス ボード、シリアル番号（BIOS ID）、アクティベーション キー値、ライセンス タイプ（R または UR）、および、コンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

show version コマンドで表示されるシリアル番号は、フラッシュ パーティション BIOS のものです。シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを取得する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

（注）　稼働時間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台の装置が動作を停止した場合、他の装置が動作を継続している限り、稼働時間の値は増加していきます。

例

次の例は、ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示する方法を示しています。

```
hostname# show version

Cisco PIX Security Appliance Software Version 7.0(4)
Device Manager Version 5.0(4)

Compiled on Tue 27-Sep-05 10:41 by root
System image file is "flash:/cdisk.bin"
Config file at boot was "startup-config"

pix2 up 7 days 7 hours

Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 0: Ext: Ethernet0           : address is 0011.2094.1d2b, irq 10
 1: Ext: Ethernet1           : address is 0011.2094.1d2c, irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Enabled
VPN Peers                   : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: 808184143
Running Activation Key: 0xcf22f25d 0xec1c3174 0x8cb138a0 0xaad8b878 0x4f32fd90
Configuration last modified by enable_15 at 14:18:26.103 UTC Thu Oct 6 2005
hostname#
```

関連コマンド

コマンド	説明
show hardware	ハードウェアの詳細情報を表示します。
show serial	ハードウェアのシリアル情報を表示します。
show uptime	セキュリティ アプライアンスが動作している期間の長さを表示します。

show vpn load-balancing

VPN ロードバランシング仮想クラスタのコンフィギュレーションに関する実行時統計情報を表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロードバランシング モードで **show vpn load-balancing** コマンドを使用します。

show vpn load-balancing

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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	•	—	•	—	—
特権 EXEC	•	—	•	—	—
VPN ロードバランシング	•	—	•	—	—

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

show vpn load-balancing コマンドは、仮想 VPN ロードバランシング クラスタに関する統計情報を表示します。ローカル デバイスが VPN ロードバランシング クラスタに参加していない場合、このコマンドは、このデバイスには VPN ロードバランシングが設定されていないことを通知します。

例

次の例は、ローカル デバイスが VPN ロードバランシング クラスタに参加している場合の **show vpn load-balancing** コマンドおよびその出力を示しています。

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
Public IP Role Pri Model Load (%) Sessions
-------------------------------------------------------------
* 192.168.1.40 Master 10 PIX-515 0 0
192.168.1.110 Backup 5 PIX-515 0 0
hostname(config-load-balancing)#
```

ローカル デバイスが VPN ロードバランシング クラスタに参加していない場合、**show vpn load-balancing** コマンドは、上とは異なる次のような結果を表示します。

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド文を削除します。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
vpn load-balancing	vpn ロードバランシング モードに入ります。

show vpn-sessiondb

VPN セッションに関する情報を表示するには、特権 EXEC モードで **show vpn-sessiondb** コマンドを使用します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できるほか、情報をフィルタリングおよびソートするためのオプションが用意されています。「シンタックスの説明」の表と「使用上のガイドライン」で、それぞれの使用可能なオプションについて説明しています。

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* **| webvpn | email-proxy} [filter {name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo***}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]**

シンタックスの説明

表示の詳細度	
detail	セッションに関する詳細な情報を表示します。たとえば、IPSec セッションに対して **detail** オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの追加の詳細情報が表示されます。 **detail** と **full** オプションを指定すると、セキュリティ アプライアンスはマシンで読み取り可能な形式で詳細出力を表示します。
filter	1 つ以上のフィルタ オプションを使用して、指定する情報のみを表示するように出力をフィルタリングします。詳細については、使用上の注意を参照してください。
full	連続した、短縮されていない出力を表示します。出力の各レコード間は、| 記号と || 文字列で区切られます。
sort	指定するソート オプションに従って出力をソートします。詳細については、使用上の注意を参照してください。
表示するセッション タイプ	
email-proxy	電子メールプロキシ セッションを表示します。電子メールプロキシ セッションに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**（接続名）、**ipaddress**（クライアント）、**encryption** を使用して情報をフィルタリングすることもできます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号（1 ～ 750）を指定します。フィルタ オプションとソート オプションは適用されません。
l2l	VPN の LAN-to-LAN セッション情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
remote	リモートアクセス セッションを表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションである **name**、**a-ipaddress**、**p-ipaddress**、**tunnel-group**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
webvpn	WebVPN セッションに関する情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**encryption** を使用して情報をフィルタリングすることもできます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード　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　次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ / ソート オプション	意味
filter a-ipaddress *IPaddr*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）についてのみ情報を表示します。
sort a-ipaddress	割り当て済み IP アドレスを基準として、表示内容をソートします。
filter encryption *encryption-algo*	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションについてのみ情報を表示します。
sort encryption	暗号化アルゴリズムを基準として、表示内容をソートします。 暗号化アルゴリズムには、次の種類があります。 aes128　des aes192　3des aes256　rc4
filter ipadddress *IPaddr*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）についてのみ情報を表示します。
sort ipaddress	内部 IP アドレスを基準として、表示内容をソートします。
filter name *username*	出力をフィルタリングして、指定したユーザ名（複数可）に関するセッションを表示します。
sort name	ユーザ名を基準として、表示内容をアルファベット順でソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスについてのみ情報を表示します。
sort p-address	指定した外部 IP アドレス（複数可）を基準として、表示内容をソートします。
filter protocol *protocol-name*	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションについてのみ情報を表示します。

フィルタ / ソート オプション	意味
sort protocol	プロトコルを基準として、表示内容をソートします。 プロトコルには、次の種類があります。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
filter tunnel-group *groupname*	出力をフィルタリングして、指定したトンネルグループ（複数可）についてのみ情報を表示します。
sort tunnel-group	トンネルグループを基準として、表示内容をソートします。
| 記号	引数 {begin | include | exclude | grep | [-v]} {reg_exp} を使用して、出力を修正します。
<cr>	出力をコンソールに送信します。

特権 EXEC モードで入力した次の例では、LAN-to-LAN セッションに関する詳細な情報を表示しています。

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.1
Index        : 1                     IP Addr      : 172.16.0.1
Protocol     : IPSecLAN2LAN          Encryption   : AES256
Bytes Tx     : 48484156              Bytes Rx     : 875049248
Login Time   : 09:32:03 est Mon Aug 2 2004
Duration     : 6:16:26
Filter Name  :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 63814 Seconds
  D/H Group    : 5

IPSec:
  Session ID   : 2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224              Bytes Rx     : 2639672
  Pkts Tx      : 1635314               Pkts Rx      : 37526


IPSec:
  Session ID   : 3
  Local Addr   : 10.0.0.1/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 6282 Seconds
  Bytes Tx     : 1619268               Bytes Rx     : 872409912
  Pkts Tx      : 19277                 Pkts Rx      : 1596809

hostname#
```

関連コマンド

コマンド	説明
show running-configuration vpn-sessiondb	VPN セッション データベースの実行コンフィギュレーションを表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。
show vpn-sessiondb summary	すべての VPN セッションの要約を表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルまたは暗号化アルゴリズムごとの比率（%）を表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

シンタックスの説明

encryption	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化について指定します。暗号化アルゴリズムには、次の種類があります。 aes128　des aes192　3des aes256　rc4
filter *groupname*	出力をフィルタリングして、指定するトンネルグループについてのみセッション比率を表示します。
protocol	表示するプロトコルを指定します。プロトコルには、次の種類があります。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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、**encryption** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio enc
Filter Group          : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions        Percent
none                     0                0%
DES                      1               20%
3DES                     0                0%
AES128                   4        80%
AES192                   0                0%
AES256                   0                0%
```

次に、**protocol** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio protocol
Filter Group          : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions        Percent
IKE                      0                0%
IPSec                    1               20%
IPSecLAN2LAN             0                0%
IPSecLAN2LANOverNatT     0                0%
IPSecOverNatT            0                0%
IPSecOverTCP             1 20%
IPSecOverUDP             0                0%
vpnLoadBalanceMgmt       0                0%
userHTTPS                0                0%
IMAP4S                   3 30%
POP3S                    0                0%
SMTPS                    3 30%
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show vpn-sessiondb summary

現在の VPN セッションの要約を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。セッションの要約は、現在のセッションの合計数、各タイプの現在のセッション数、ピーク時のセッション数および累積合計セッション数、最大同時セッション数を含んでいます。

show vpn-sessiondb summary

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 vpn-sessiondb summary** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb summary

Active Sessions:                Session Information:
  LAN-to-LAN : 2                    Peak Concurrent : 7
  Remote Access : 5                 Concurrent Limit: 2000
  WebVPN : 0                        Cumulative Sessions: 12
  Email Proxy : 0
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show xlate

変換スロットに関する情報を表示するには、特権 EXEC モードで **show xlate** コマンドを使用します。

show xlate [***global*** *ip1*[**-***ip2*] [***netmask*** *mask*]] [***local*** *ip1*[**-***ip2*] [***netmask*** *mask*]][***gport*** *port1*[**-***port2*]] [***lport*** *port1*[**-***port2*]] [***interface*** *if_name*] [***state*** *state*] [***debug***] [***detail***]

show xlate ***count***

シンタックスの説明

count	変換の数を表示します。
debug	（オプション）変換のデバッグ情報を表示します。
detail	（オプション）変換の詳細情報を表示します。
global *ip1*[**-***ip2*]	（オプション）アクティブな変換をグローバル IP アドレス（またはアドレス範囲）別に表示します。
gport *port1*[**-***port2*]	アクティブな変換をグローバル ポート（またはポート範囲）別に表示します。
interface *if_name*	（オプション）アクティブな変換をインターフェイス別に表示します。
local *ip1*[**-***ip2*]	（オプション）アクティブな変換をローカル IP アドレス（またはアドレス範囲）別に表示します。
lport *port1*[**-***port2*]	アクティブな変換をローカルポート(またはポート範囲)別に表示します。
netmask *mask*	（オプション）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（オプション）アクティブな変換を状態別に表示します。次の状態を 1 つまたは複数入力できます。 • ***static*** : **static** 変換を指定します。 • ***portmap*** : PAT グローバル変換を指定します。 • ***norandomseq*** : ***norandomseq*** の設定を使用した **nat** 変換または **static** 変換を指定します。 • ***identity*** : **nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をカンマで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

show xlate コマンドは、変換スロットの内容を表示します。**show xlate detail** コマンドは、次の情報を表示します。

- {**ICMP**|**TCP**|**UDP**} **PAT from** *interface*:*real-address*/*real-port* **to** *interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*
- **NAT from** *interface*:*real-address*/*real-port to interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*

表 7-29 は、変換フラグを説明しています。

表 7-29　変換フラグ

フラグ	説明
s	スタティック変換スロット
d	次のクリーニング サイクルでのダンプ変換スロット
r	ポート マップ変換（ポート アドレス変換）
n	TCP シーケンス番号の非ランダム化
i	内部アドレス変換
D	DNS A RR リライト
I	**nat 0** からの識別変換

（注）　**vpnclient** コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合は、**show xlate** コマンドにより、スタティック変換用の xlate が複数表示されることがあります。

例

次に、**show xlate** コマンドの出力例を示します。この例では、3 つのアクティブな PAT の変換スロットの情報が表示されています。

```
hostname# show xlate

3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

次に、**show xlate detail** コマンドの出力例を示します。この例では、3 つのアクティブな PAT の変換タイプとインターフェイスの情報が表示されています。

最初のエントリは、内部ネットワーク上のホストポート（10.1.1.15, 1026）から外部ネットワーク上のホストポート（192.150.49.1, 1024）への TCP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレスポートに適用されることを示しています。

2 番目のエントリは、内部ネットワーク上のホストポート（10.1.1.15, 1028）から外部ネットワーク上のホストポート（192.150.49.1, 1024）への UDP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレスポートに適用されることを示しています。

3 番目のエントリは、内部ネットワーク上のホスト ICMP ID（10.1.1.15, 21505）から外部ネットワーク上のホスト ICMP ID（192.150.49.1, 0）への ICMP PAT です。r フラグは、変換が PAT であることを示しています。i フラグは、変換が内部アドレス ICMP ID に適用されることを示しています。

内部アドレス フィールドは、高セキュリティ インターフェイスから低セキュリティ インターフェイスに移動するパケットに送信元アドレスとして表示されます。低セキュリティ インターフェイスから高セキュリティ インターフェイスに移動するパケットでは、内部アドレス フィールドが宛先アドレスとして表示されます。

```
hostname# show xlate detail

3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

次に、**show xlate** コマンドの出力例を示します。この例では、2 つのスタティック変換が表示されています。最初の変換には「nconns」という接続が 1 つ関連付けられ、2 番目の変換には 4 つ関連付けられています。

```
hostname# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

関連コマンド

コマンド	説明
clear xlate	現在の変換情報と接続情報を消去します。
show conn	アクティブな接続をすべて表示します。
show local-host	ローカル ホストのネットワーク情報を表示します。
show uauth	現在の認証済みユーザを表示します。

shun

新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにするには、特権 EXEC モードで **shun** コマンドを使用します。セキュリティ アプライアンスが排除のルックアップに使用する実際のアドレス（*src_ip*）に基づく排除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。

shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *src_ip* [**vlan** *vlan_id*]

シンタックスの説明

dest_port	（オプション）排除を引き起こす接続の宛先ポート。
dst_ip	（オプション）ターゲット ホストのアドレス。
protocol	（オプション）UDP や TCP などの IP プロトコル。*dst_ip* を指定する場合は必須です。
src_ip	攻撃ホストのアドレス。
src_port	（オプション）排除を引き起こす接続の送信元ポート。
vlan_id	（オプション）VLAN ID 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。

コマンドのモード

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。

使用上のガイドライン

shun コマンドを使用すると、攻撃を受けるインターフェイスにブロッキング機能を適用できます。攻撃ホストの IP 送信元アドレスを含むパケットは、ブロッキング機能が手動でまたは Cisco IPS マスター モジュールによって削除されるまで、ドロップされ記録されます。IP 送信元アドレスからのトラフィックはセキュリティ アプライアンスを通過できません。残っている接続はすべて、標準アーキテクチャの一部としてタイムアウトになります。**shun** コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブであるかどうかに関らず適用されます。

ホストの送信元 IP アドレスだけを指定して **shun** コマンドを使用する場合、デフォルトは 0 となります。攻撃ホストからのトラフィックは許可されません。

shun コマンドは、攻撃のダイナミックなブロックに使用されるため、セキュリティ アプライアンス コンフィギュレーションには表示されません。

インターフェイスを削除すると、そのインターフェイスに適用されている排除もすべて削除されます。新しいインターフェイスを追加する場合や、同じインターフェイス（同じ名前）を置き換える場合、そのインターフェイスを IPS センサーで監視するときは、そのインターフェイスを IPS センサーに追加する必要があります。

例

次の例は、攻撃ホスト（10.1.1.27）が TCP で攻撃対象（10.2.2.89）との接続を作成していることを示しています。接続は、セキュリティ アプライアンス接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

shun コマンドを次のように適用したとします。

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

上のコマンドにより、セキュリティ アプライアンス接続テーブルから接続が削除され、10.1.1.27 からのパケットがセキュリティ アプライアンスを通過できなくなります。攻撃ホストは、セキュリティ アプライアンスの内部にある場合も、外部にある場合もあります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
show shun	排除情報を表示します。

shutdown

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

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

物理インターフェイスは、デフォルトではすべてシャットダウンされます。セキュリティ コンテキスト内の割り当て済みインターフェイスは、コンフィギュレーション内ではシャットダウンされません。

コマンドのモード

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、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

例

次の例では、メインのインターフェイスをイネーブルにしています。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
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
```

次の例では、サブインターフェイスをイネーブルにしています。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、サブインターフェイスをシャットダウンしています。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に関するすべての変換をリセットして、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。

smtps

SMTPS コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンド モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。SMTPS は、SSL 接続を通じた電子メール送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

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。

コマンドのモード

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。

例

次の例は、SMTPS コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# smtps
hostname(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバを設定するには、グローバル コンフィギュレーション モードで **smtp-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 アプライアンスには、特定のイベントが発生したことを外部エンティティに通知するときにイベント システムが使用できる、内部 SMTP クライアントが含まれています。これらのイベント通知を SMTP サーバで受信して、指定した電子メール アドレスに転送するように SMTP サーバを設定することができます。SMTP ファシリティがアクティブになるのは、セキュリティ アプライアンスで電子メール イベントをイネーブルにしている場合のみです。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

シンタックスの説明

primary_server	プライマリ SMTP サーバを指定します。IP アドレスまたは DNS 名のいずれかを使用します。
backup_server	プライマリ SMTP サーバが使用不能になった場合に、イベント メッセージのリレー先となるバックアップ SMTP サーバを指定します。IP アドレスまたは DNS 名のいずれかを使用します。

デフォルト

デフォルトでは、SMTP サーバは設定されていません。

コマンドのモード

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。

例

次の例は、SMTP サーバの IP アドレスとして 10.1.1.24 を設定し、バックアップ SMTP サーバの IP アドレスとして 10.1.1.34 を設定する方法を示しています。

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-server

セキュリティ アプライアンスのイベント情報を SNMP で提供するには、特権 EXEC モードで **snmp-server** コマンドを使用します。SNMP 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。

snmp-server {community | contact | location} *text*}

no snmp-server {community | contact | location} *text*}

snmp-server host *interface_name ip_addr* **[community** *commstr*] [**trap | poll**] [***version vers***] [***udp-port udp_port***]

no snmp-server host *interface_name ip_addr* **[community** *commstr*] [**trap | poll**] [***version vers***] [***udp-port udp_port***]

snmp-server enable [traps [***all*** | ***feature*** [***trap1*** ... [***trapn***]]]

no snmp-server enable [traps [***all*** | ***feature*** [***trap1*** ... [***trapn***]]]

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

シンタックスの説明

community *text*	SNMP 管理ステーションに対するセキュリティ アプライアンスのコミュニティ ストリングを指定します。
contact *text*	連絡先の担当者または PIX システム管理者の名前を指定します。
location *text*	セキュリティ アプライアンスの場所を指定します。
host	トラップの送信先または SNMP 要求の送信元である SNMP 管理ステーションの IP アドレスを指定します。
interface_name	SNMP 管理ステーションが存在するインターフェイス名。
ip_addr	SNMP トラップの送信先または SNMP 要求の送信元であるホストの IP アドレス。
trap	（オプション）トラップのみが送信され、このホストはポーリングを実行できないことを指定します。
poll	（オプション）このホストがポーリングを実行できることを指定します。
enable	特定の SNMP トラップ通知をイネーブルにします。
enable traps	SNMP トラップ通知としてのログ メッセージの送信をイネーブルにします。
all	すべての機能に関するトラップをイネーブルまたはディセーブルにします。
community	セキュリティ アプライアンスのコミュニティ ストリングを指定します。
commstr	特定のホストのコミュニティ ストリング。
feature	トラップをイネーブルにする対象となる機能。
trapn	イネーブルにする特定のトラップ。
listen-port	着信 SNMP 要求用のデフォルト ポート（161）を上書きします。
lport	着信要求を受け入れるポート。
udp-port *udp_port*	通知の送信先となるポートを設定します。

デフォルト

デフォルトでは、トラップとポールの両方が有効です。

コマンドのモード

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。

使用上のガイドライン

snmp-server コマンドを使用すると、サイト、管理ステーション、コミュニティ ストリング、およびユーザ情報を識別できます。

SNMP 管理ステーションで使用するパスワード キーを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと、管理されているネットワーク ノードとの間での共有秘密です。セキュリティ アプライアンスは、キーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、サイトにコミュニティ ストリングを指定してから、ルータ、セキュリティ アプライアンス、および管理ステーションに同じストリングを設定できます。セキュリティ アプライアンスはこのストリングを使用しますが、無効なコミュニティ ストリングを持つ要求には応答しません。

contact *text* は、大文字と小文字が区別される最大 127 文字の値です。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

location *text* は、大文字と小文字が区別される最大 127 文字の値です。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

最大 32 個の SNMP 管理ステーションを指定できます。

snmp-server host コマンドを使用してホストを設定するときに、***trap*** オプションを指定すると、デバイスは当該ホストからの着信要求を拒否するようになります。

clear configure snmp-server コマンドおよび **no snmp-server** コマンドは、次のように、コンフィギュレーション内で SNMP コマンドをディセーブルにします。

```
hostname(config)# no snmp-server location
hostname(config)# no snmp-server contact
hostname(config)# snmp-server community public
hostname(config)# no snmp-server enable traps
```

例

次の例は、管理ステーションから SNMP 要求を受信し始めるために入力するコマンドを示しています。

```
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
```

関連コマンド

コマンド	説明
clear configure snmp-server	簡易ネットワーク管理プロトコル（SNMP）サーバをディセーブルにします。
show snmp-server statistics	SNMP サーバに関する情報を表示します。
show running-config snmp-server	SNMP サーバのコンフィギュレーションを表示します。

snmp-map

SNMP 検査のパラメータを定義している特定のマップを指定するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map *map_name*

no snmp-map *map_name*

シンタックスの説明

map_name	SNMP 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。

コマンドのモード

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

snmp-map コマンドは、SNMP 検査のパラメータを定義している特定のマップを指定するために使用します。このコマンドを入力すると、システムが SNMP マップ コンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップを定義した後は、**inspect snmp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

例

次の例は、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

snmp-server enable trap remote-access

しきい値に基づくトラップ送信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 **snmp-server enable trap remote-access** コマンドを使用します。しきい値に基づくトラップ送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。このコマンドを使用すると、リモートアクセス セッションが **remote-access threshold session-threshold-exceeded** コマンドで設定した数に達したときに、セキュリティ アプライアンスでトラップを送信できます。

snmp-server enable trap remote-access session-threshold-exceeded

no **snmp-server enable trap remote-access**

シンタックスの説明

session-threshold-exceeded	セッションしきい値を超えています。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

例

次の例は、しきい値に基づくトラップ送信をイネーブルにする方法を示しています。

```
hostname# snmp-server enable trap remote-access session-threshold-exceeded
```

関連コマンド

コマンド	説明
remote-access threshold session-threshold-exceeded	アクティブな同時リモートアクセス セッションの数を指定します。この数に達すると、セキュリティ アプライアンスがトラップを送信します。

speed

銅線（RJ-45）イーサネット インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度の設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed {***auto*** | ***10*** | ***100*** | ***1000*** | ***nonegotiate***}

no speed [***auto*** | ***10*** | ***100*** | ***1000*** | ***nonegotiate***]

シンタックスの説明

10	速度を 10BASE-T に設定します。
100	速度を 100BASE-T に設定します。
1000	速度を 1000BASE-T に設定します（銅線ギガビット イーサネットの場合のみ）。
auto	速度を自動検出します。
nonegotiate	ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータはネゴシエートしないでください。ファイバ インターフェイスに対して使用できる設定は、このコマンド、およびこのコマンドの **no** 形式のみです。この値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスはリンクのネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。

デフォルト

銅線インターフェイスの場合、デフォルトは **speed auto** です。

ファイバ インターフェイスの場合、デフォルトは **no speed nonegotiate** です。

コマンドのモード

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、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

速度は、物理インターフェイスに対してのみ設定します。

ネットワークが自動検出をサポートしていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式のいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックス方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

例

次の例では、速度を 1000BASE-T に設定しています。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
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
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
duplex	デュプレックス モードを設定します。
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。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

split-dns

スプリット トンネルを介して解決されるドメインのリストを入力するには、グループポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。**split-dns none** コマンドを発行して作成されたヌル リストを含めて、設定済みのスプリット トンネリング ドメインのリストがすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルト グループポリシーに含まれているリストを継承します。ユーザがこれらのスプリット トンネリング ドメイン リストを継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

シンタックスの説明

value *domain-name*	スプリット トンネルを介してセキュリティ アプライアンスが解決するドメインの名前を提供します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストにヌル値を設定して、スプリット DNS リストを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーからスプリット DNS リストを継承しないようにします。

デフォルト

スプリット DNS はディセーブルです。

コマンドのモード

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

ドメインのリストに記述する各エントリは、1 個のスペースを使用して区切ります。エントリの数に制限はありませんが、エントリ文字列の長さは、255 文字を超えることはできません。使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

no spilit-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成されたヌル値を含めて、現在の値がすべて削除されます。

例

次の例は、FirstGroup というグループポリシーに対して、スプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセスリストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-tunnel-network-list

スプリット トンネリング用のネットワークのリストを作成するには、グループポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワークのリストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ネットワークのリストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含めて、設定済みのネットワーク リストがすべて削除されます。

スプリット トンネリング ネットワークのリストがない場合、ユーザは、デフォルト グループポリシーまたは指定したグループポリシーに含まれているネットワーク リストを継承します。ユーザがこれらのネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワークのリストは、トラフィックにトンネルの通過を要求するネットワークと、トンネリングを要求しないネットワークとを区別するためのものです。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

シンタックスの説明

value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙したアクセスリストを指定します。
none	スプリット トンネリング用のネットワークのリストが存在しないことを指定します。セキュリティ アプライアンスは、すべてのトラフィックをトンネリングします。 スプリット トンネリング ネットワークのリストにヌル値を設定して、スプリット トンネリングを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーから、スプリット トンネリング ネットワークのデフォルトのリストを継承しないようにします。

デフォルト

デフォルトでは、スプリット トンネリング ネットワークのリストはありません。

コマンドのモード　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　セキュリティ アプライアンスは、スプリット トンネリングを実行するかどうかをネットワーク リストに基づいて判断します。このリストは、プライベート ネットワーク上にあるアドレスのリストで構成される、標準的な ACL です。

no spilit-tunnel-network-list コマンドを引数なしで使用すると、**split-tunnel-network-list none** コマンドを発行して作成されたヌル値を含めて、現在のネットワーク リストがすべて削除されます。

例　次の例は、FirstGroup というグループポリシーに対して、FirstList というネットワーク リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセスリストを作成します。または、ダウンロード可能なアクセスリストを使用します。
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。split-tunnel-policy の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。このコマンドを使用すると、スプリット トンネリングの値を別のグループポリシーから継承できます。

スプリット トンネリングを利用すると、リモートアクセス IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようになります。スプリット トンネリングがイネーブルになっている場合、宛先が IPSec トンネルの向こう側ではないパケットについては、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが不要です。

このコマンドは、このようなスプリット トンネリング ポリシーを特定のネットワークに適用するものです。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

シンタックスの説明

excludespecified	トラフィックを暗号化なしで送信する宛先ネットワークのリストを定義します。この機能が役立つのは、企業ネットワークにトンネル経由で接続しながら、ローカル ネットワーク上のプリンタなどのデバイスにアクセスしようとするリモート ユーザです。このオプションが適用されるのは、Cisco VPN Client のみです。
split-tunnel-policy	トラフィックのトンネリング規則を設定することを指定します。
tunnelall	トラフィックを暗号化なしでは送信しないこと、またはセキュリティ アプライアンス以外の宛先に送信しないことを指定します。リモート ユーザは、インターネット ネットワークには企業ネットワークを通じて到達し、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークからのトラフィック、または指定したネットワークに向かうトラフィックをすべてトンネリングします。このオプションを指定すると、スプリット トンネリングがイネーブルになります。これによって、トンネリングの対象となるネットワークのアドレス リストを作成できるようになります。他のアドレス宛てのデータは、すべて暗号化なしで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

デフォルト（tunnelall）では、スプリット トンネリングはディセーブルです。

コマンドのモード

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

スプリット トンネリングは、本来はセキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことをお勧めします。

例

次の例は、FirstGroup というグループポリシーに対して、指定したネットワークのみトンネリングするスプリット トンネリング ポリシーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリング用のアクセスリストが存在しないことを指定します。トラフィックは、すべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセスリストを指定します。

ssh

セキュリティ アプライアンスへの SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。セキュリティ アプライアンスへの SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

シンタックスの説明

interface	SSH をイネーブルにするセキュリティ アプライアンス インターフェイス。指定しない場合は、外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 SSH がイネーブルになります。
ip_address	セキュリティ アプライアンスへの SSH 接続の開始が認可されるホストまたはネットワークの IPv4 アドレス。ホストの場合は、ホスト名を入力することもできます。
ipv6_address/prefix	セキュリティ アプライアンスへの SSH 接続の開始が認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

ssh *ip_address* コマンドは、セキュリティ アプライアンスへの SSH 接続の開始を認可するホストまたはネットワークを指定します。複数の ssh コマンドをコンフィギュレーションに含めることができます。このコマンドの **no** 形式は、特定の ssh コマンドをコンフィギュレーションから削除します。すべての ssh コマンドを削除するには、**clear configure ssh** コマンドを使用します。

SSH を使用してセキュリティ アプライアンスに接続するには、**crypto key generate rsa** コマンドを使用して、デフォルトの RSA キーをあらかじめ生成しておく必要があります。

セキュリティ アプライアンスでは、次のセキュリティ アルゴリズムと暗号がサポートされています。

- データ暗号化のための 3DES 暗号と AES 暗号
- パケットの完全性を保証するための HMAC-SHA アルゴリズムと HMAC-MD5 アルゴリズム
- ホスト認証のための RSA 公開キー アルゴリズム

- キー交換のための Diffie-Hellman Group 1 アルゴリズム

セキュリティ アプライアンスでは、次の SSH バージョン 2 機能はサポートされていません。

- X11 転送
- ポート転送
- SFTP サポート
- Kerberos と AFS のチケットの引き渡し
- データ圧縮

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
crypto key generate rsa	ID 証明書のための RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

シンタックスの説明

session_id	ID 番号で指定した SSH セッションを切断します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次の例は、SSH セッションが切断されるようすを示しています。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh scopy enable

セキュリティ アプライアンス上でセキュア コピー（SCP）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 **ssh scopy enable** コマンドを使用します。SCP 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。

ssh scopy enable

no ssh scopy enable

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

SCP は、サーバ専用の実装です。SCP のための接続を受け入れること、および終了することはできますが、開始することはできません。セキュリティ アプライアンスでは、次の制限事項があります。

- SCP のこの実装では、ディレクトリをサポートしていないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスのみ実行できます。
- SCP 使用時は、バナーをサポートしていません。
- SCP はワイルドカードをサポートしません。
- SSH バージョン 2 接続をサポートするには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が含まれている必要があります。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

シンタックスの説明

number	SSH セッションが切断されるまでに非アクティブ状態を維持する時間（分）を指定します。有効な値は 1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は 5 分です。

コマンドのモード

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

ssh timeout コマンドは、セッションが切断されるまでにアイドル状態を維持する時間（分）を指定します。デフォルトの時間は 5 分です。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続のみを受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

セキュリティ アプライアンスが受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。デフォルト値では、セキュリティ アプライアンスへの SSH バージョン 1 接続と SSH バージョン 2 接続が許可されます。

ssh version {*1* | *2*}

no ssh version [*1* | *2*]

シンタックスの説明

1	SSH バージョン 1 接続のみをサポートすることを指定します。
2	SSH バージョン 2 接続のみをサポートすることを指定します。

デフォルト

デフォルトでは、SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。

コマンドのモード

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

1 と 2 は、セキュリティ アプライアンスが使用する SSH のバージョンをいずれかに限定するように指定します。このコマンドの **no** 形式は、セキュリティ アプライアンスをデフォルトの状態である互換モード（両方のバージョンを使用可能）に戻します。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

ssl client-version

セキュリティ アプライアンスがクライアントとして動作するときに使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl client-version** コマンドを使用します。デフォルトの **any** に戻すには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが送信する SSL/TLS のバージョンを限定できます。

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 のみを受け入れます。
tlsv1-only	セキュリティ アプライアンスは、TLS バージョン 1 クライアントの hello を送信し、TLS バージョン 1 のみを受け入れます。

デフォルト

デフォルト値は、**any** です。

コマンドのモード

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

TCP ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

問題となるのは、ポート転送アプリケーションを起動したときに、Java はクライアントの Hello パケットで SSLv3 のみをネゴシエートする点です。

例

次の例は、SSL クライアントとして動作するときに、TLSv1 のみを使用して通信するようにセキュリティ アプライアンスを設定する方法を示しています。

```
hostname(config)# ssl client-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl encryption

SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。このコマンドをもう一度発行すると、直前の設定が上書きされます。アルゴリズムを使用する優先順位は、アルゴリズムの順序によって決まります。アルゴリズムを追加または削除して、使用している環境での要件を満たすようにしてください。デフォルト（すべての暗号化アルゴリズムが使用可能）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*possibly others*]

no ssl encryption

シンタックスの説明

3des-sha1	Secure Hash Algorithm 1 を使用する Triple DES 暗号化を指定します。
des-sha1	Secure Hash Algorithm 1 を使用する DES 暗号化を指定します。
rc4-md5	MD5 ハッシュ関数を使用する RC4 暗号化を指定します。
possibly others	暗号化アルゴリズムが、将来のリリースで追加される可能性があることを示します。

デフォルト

デフォルトでは、すべてのアルゴリズムが次の順序で使用可能になっています。

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

コマンドのモード

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。

例

次の例は、3des-sha1 暗号化アルゴリズムと des-sha1 暗号化アルゴリズムを使用するようにセキュリティ アプライアンスを設定する方法を示しています。

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl server-version

セキュリティ アプライアンスがサーバとして動作するときに使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが受け入れる SSL/TLS のバージョンを限定できます。

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 をネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 クライアントの hello のみを受け入れ、SSL バージョン 3 のみを使用します。
tlsv1	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、TLS バージョン 1 をネゴシエートします。
tlsv1-only	セキュリティ アプライアンスは、TLSv1 クライアントの hello のみを受け入れ、TLS バージョン 1 のみを使用します。

デフォルト

デフォルト値は、**any** です。

コマンドのモード

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

TCP ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

電子メールプロキシを設定する場合は、SSL バージョンを tlsv1-only に設定しないでください。Outlook と Outlook Express は、TLS をサポートしていません。

例

次の例は、SSL サーバとして動作するときに、TLSv1 のみを使用して通信するようにセキュリティアプライアンスを設定する方法を示しています。

```
hostname(config)# ssl server-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている ssl コマンドのセットを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書トラストポイントを指定するには、グローバル コンフィギュレーション モードで **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイスに使用される、フォールバック トラストポイントが作成されます。インターフェイスの指定がない SSL トラストポイン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。インターフェイスの指定がないエントリを削除するには、このコマンドの **no ssl trust-point** {*trustpoint [interface]*} 形式を使用します。

ssl trust-point {*trustpoint [interface]*}

no ssl trust-point

シンタックスの説明

interface	トラストポイントを適用するインターフェイス名。このインターフェイス名は、**nameif** コマンドで指定したものです。
trustpoint	**crypto ca trustpoint** {*name*} コマンドで設定した、CA トラストポイントの *name*。

デフォルト

トラストポイントの関連付けはありません。セキュリティ アプライアンスは、デフォルトの自己生成 RSA キーペア証明書を使用します。

コマンドのモード

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

このコマンドを使用する場合は、次の注意事項に従ってください。

- *trustpoint* の値は、**crypto ca trustpoint {*name*}** コマンドで設定した CA トラストポイントの名前にする必要があります。
- *interface* の値は、事前設定済みのインターフェイスの *nameif* 名にする必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照している **ssl trust-point** エントリもすべて削除されます。
- **ssl trustpoint** エントリは、インターフェイスごとに 1 つずつ、およびインターフェイスの指定がないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。

次の例は、このコマンドの **no** 形式を使用する方法を示しています。

このコンフィギュレーションには、次の SSL トラストポイントが含まれています。

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

次のコマンドを発行します。

```
no ssl trust-point
```

show run ssl を実行すると、次のように表示されます。

```
ssl trust-point tp2 outside
```

例

次の例は、内部インターフェイス用の FirstTrust という SSL トラストポイント、および関連するインターフェイスを持たない DefaultTrust というトラストポイントを設定する方法を示しています。

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

次の例は、このコマンドの **no** 形式を使用して、関連するインターフェイスを持たないトラストポイントを削除する方法を示しています。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

次の例は、インターフェイスが関連付けられているトラストポイントを削除する方法を示しています。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。

static

実際の IP アドレスをマッピング IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定するには、グローバル コンフィギュレーション モードで **static** 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。

スタティック NAT の場合：

static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [**norandomseq** [***nailed***]] [[**tcp**] {*max_conns* {*emb_lim*}} [**udp** *udp_max_conns*]]

no static (*real_ifc*,***mapped_ifc***) {***mapped_ip*** | **interface**} {***real_ip*** [**netmask** ***mask***] | **access-list** ***access_list_name***} [**dns**] [**norandomseq** [***nailed***]] [[**tcp**] {***max_conns*** {***emb_lim***}} [**udp** ***udp_max_conns***]]

スタティック PAT の場合：

static (*real_ifc*,***mapped_ifc***) {**tcp** | **udp**} {***mapped_ip*** | **interface**} *mapped_port* {***real_ip real_port*** [**netmask** ***mask***]} | {**access-list** ***access_list_name***} [**dns**] [**norandomseq** [***nailed***]] [[**tcp**] {***max_conns*** {***emb_lim***}} [**udp** ***udp_max_conns***]]

no static (*real_ifc*,***mapped_ifc***) {**tcp** | **udp**} {***mapped_ip*** | **interface**} *mapped_port* {***real_ip real_port*** [**netmask** ***mask***]} | {**access-list** ***access_list_name***} [**dns**] [**norandomseq** [***nailed***]] [[**tcp**] {***max_conns*** {***emb_lim***}} [**udp** ***udp_max_conns***]]

シンタックスの説明

access-list *access_list_name*	実際のアドレスと宛先アドレス（またはポート）を指定して、NAT 用の実際のアドレスを指定できます。この機能は、ポリシー NAT と呼ばれます。 アクセスリストで使用されるサブネット マスクは、*mapped_ip* でも使用されます。 アクセスリストには、**permit** 文のみ含めることができます。**eq** 演算子を使用して、実際のポートと宛先ポートをアクセスリスト内で指定することもできます。ポリシー NAT の場合、**inactive** キーワードと **time-range** キーワードは考慮されません。ポリシー NAT のコンフィギュレーションでは、すべての ACE はアクティブであるものと見なされます。
dns	（オプション）DNS 応答に含まれていて、このスタティック エントリと一致する A レコード（アドレス レコード）を書き換えます。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。

emb_lim	（オプション）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。 このオプションは、外部 NAT には適用されません。TCP 代行受信機能が適用されるのは、よりセキュリティ レベルの高いホストまたはサーバのみです。外部 NAT に対して初期接続の制限を設定しても、その初期接続制限は無視されます。
interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。 **（注）** インターフェイスの IP アドレスをスタティック PAT エントリに含める場合は、実際の IP アドレスを指定するのではなく、interface キーワードを使用する必要があります。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip	実際のアドレスの変換後のアドレスを指定します。
mapped_port	マッピング TCP ポートまたは UDP ポートを指定します。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
nailed	（オプション）非対称ルーティング トラフィックの TCP セッションを許容します。このオプションを指定すると、着信トラフィックは、対応する発信接続の状態が確立されていなくてもセキュリティ アプライアンスを通過することができます。**failover timeout** コマンドと共に使用します。**failover timeout** コマンドは、システムがブートしたときまたはアクティブになったときを起点として、ネイリングされたセッションが受け入れられる期間を指定するものです。設定しない場合は、接続を再確立できません。 **（注）** **static** コマンドに ***nailed*** オプションを付加すると、当該の接続については TCP の状態追跡とシーケンス確認が省略されます。非対称ルーティングのサポートを設定する場合は、**asr-group** コマンドを使用するほうが **static** コマンドに ***nailed*** オプションを付加して使用するよりもセキュリティ上安全であり、非対称ルーティングのサポートの設定にはこの方法をお勧めします。
netmask *mask*	実際のアドレスとマッピング アドレスのサブネット マスクを指定します。単一ホストの場合は、255.255.255.255 を使用します。マスクを入力しない場合は、IP アドレス クラスのデフォルト マスクが使用されます。ただし、例外が 1 つあります。マスク後のホストビットが 0 でない場合は、ホスト マスクの 255.255.255.255 が使用されます。*real_ip* の代わりに **access-list** キーワードを使用すると、アクセスリストで使用されるサブネット マスクが *mapped_ip* にも使用されます。

norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは、外部 NAT には適用されません。ファイアウォールがランダム化するのは、セキュリティの高いインターフェイスに対してホストまたはサーバが生成する ISN のみです。外部 NAT に対して **norandomseq** を設定しても、その **norandomseq** キーワードは無視されます。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実際のアドレスを指定します。
real_port	実際の TCP ポートまたは UDP ポートを指定します。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
tcp	スタティック PAT の場合に、プロトコルを TCP として指定します。
tcp *max_conns*	サブネット全体に関して、同時 TCP 接続と UDP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します。アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトが経過すると閉じられます。 このオプションは、外部 NAT には適用されません。セキュリティ アプライアンスが追跡するのは、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に向かう接続のみです。
udp	スタティック PAT の場合に、プロトコルを UDP として指定します。
udp *udp_max_conns*	（オプション）**udp** キーワードとともに使用して、各 *real_ip* ホストが使用できる同時 UDP 接続の最大数を設定します。

デフォルト

デフォルトは次のとおりです。

- 初期接続の制限はありません。
- 接続の制限はありません。

コマンドのモード

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

スタティック NAT では、実際のアドレス（複数可）からマッピング アドレス（複数可）への固定的な変換を作成します。ダイナミック NAT およびダイナミック PAT の場合、後続の変換では、各ホストはそれぞれ別のアドレスまたはポートを使用します。スタティック NAT では、マッピング アドレスは連続する各接続で同じであり、恒久的な変換規則が存在します。このため、スタティック NAT を利用する場合は、宛先ネットワーク上のホストが変換後のホストに向かうトラフィックを開始できます（この処理を許可するアクセスリストが存在する場合）。

ダイナミック NAT と、スタティック NAT のアドレス範囲との主な違いは、スタティック NAT を利用する場合、変換後のホストに向かう接続をリモート ホストが開始できることです（この処理を許可するアクセスリストが存在する場合）。ダイナミック NAT の場合はできません。また、スタティック NAT では、実際のアドレスと同じ数のマッピング アドレスが必要になります。

スタティック PAT はスタティック NAT と同じですが、実際のアドレスおよびマッピング アドレスに対して、プロトコル（TCP または UDP）とポートを指定できる点が異なります。

この機能を使用すると、同じマッピング アドレスを複数のさまざまな static 文に対して指定できます。ただし、それぞれの文でポートが異なっている必要があります（複数のスタティック NAT 文に対して同じマッピング アドレスを使用することはできません）。

同じ実際のアドレスまたはマッピング アドレスを、複数の **static** コマンド内で同じ 2 つのインターフェイスに関して使用することはできません。同じマッピング インターフェイスに対して **global** コマンドでも定義されているマッピング アドレスは、**static** コマンドの中では使用しないでください。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

NAT は、従来の意味では、透過ファイアウォール モードで使用できません。透過ファイアウォール モードでは、***static*** コマンドを使用することによって、最大接続数、最大初期接続数、および TCP シーケンスのランダム化を設定できます。この場合、実際の IP アドレスとマッピング IP アドレスは両方とも同じです。

最大接続数、最大初期接続数、および TCP シーケンスのランダム化は、**set connection** コマンドを使用して設定することもできます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセスリストを設定する必要があります。

static コマンド文を変更または削除した後は、**clear xlate** コマンドを使用して変換を消去してください。

例

スタティック NAT の例

次のポリシー スタティック NAT の例は、宛先アドレスに応じて 2 つのマッピング アドレスに変換される 1 つの実際のアドレスを示しています。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドでは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングしています。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

次のコマンドでは、外部 IP アドレス（209.165.201.15）を内部 IP アドレス（10.1.1.6）にマッピングしています。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

次のコマンドでは、サブネット全体をスタティックにマッピングしています。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

次の例は、限定された数のユーザが、Intel Internet Phone、CU-SeeMe、CU-SeeMe Pro、MeetingPoint、または Microsoft NetMeeting を使用して、H.323 経由でコール インできるようにする方法を示しています。**static** コマンドでは、アドレス 209.165.201.0 ～ 209.165.201.30 がローカル アドレス 10.1.1.1 ～ 10.1.1.30 にマッピングされます（209.165.201.1 は 10.1.1.1 にマッピングされ、209.165.201.10 は 10.1.1.10 にマッピングされ、他も同様にマッピングされます）。

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask
255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq
h323
hostname(config)# access-group acl_out in interface outside
```

次の例は、Mail Guard をディセーブルにするためのコマンドを示しています。

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

この例では、**static** コマンドでグローバル アドレスをセットアップして、外部のホストが dmz1 インターフェイス上の 10.1.1.1 メール サーバ ホストにアクセスすることを許可します。DNS 用の MX レコードが 209.165.201.1 アドレスを指すように設定する必要があり、これによってメールはこのアドレスに送信されます。**access-list** コマンドによって、外側ユーザが SMTP ポート（25）を経由して、グローバル アドレスにアクセスできるようにしています。**no fixup protocol** コマンドにより、Mail Guard がディセーブルになります。

スタティック PAT の例

たとえば、10.1.3.0 ネットワーク上のホストから開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう Telnet トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）にリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

10.1.3.0 ネットワーク上のホストから開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう HTTP トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）にリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

セキュリティ アプライアンスの外部インターフェイス（10.1.2.14）からの Telnet トラフィックを内部ホスト 10.1.1.15 にリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

上の実際の Telnet サーバが接続を開始することを許可するには、変換を追加する必要があります。たとえば、他のすべてのタイプのトラフィックを変換するには、次のコマンドを入力します。元のままの **static** コマンドは、このサーバに向かう Telnet に関する変換を定義しています。それに対して、**nat** コマンドと **global** コマンドでは、このサーバからの発信接続に関する PAT を定義しています。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

すべての内部トラフィックに独自の変換を定義していて、内部ホストが Telnet サーバとは別のマッピング アドレスを使用している場合でも、Telnet サーバから開始されるトラフィックについては、サーバに向かう Telnet トラフィックを許可する **static** 文と同じマッピング アドレスを使用するように設定することができます。Telnet サーバにのみ適用する、より限定的な **nat** コマンドを作成する必要があります。**nat** 文は、最もよく一致しているものが読み取られます。このため、限定的な **nat** コマンドは汎用の文よりも先に一致します。次の例は、Telnet に関する **static** 文、Telnet サーバから開始されるトラフィックに関する限定的な **nat** 文、および別のマッピング アドレスを使用するその他の内部ホストに関する文を示しています。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

既知のポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションから **static** コマンドを削除します。
clear xlate	すべての変換を消去します。
nat	ダイナミック NAT を設定します。
show running-config static	コンフィギュレーションに含まれているすべての **static** コマンドを表示します。
timeout conn	接続のタイムアウトを設定します。

strict-http

HTTP に準拠しないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能の動作をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog を生成します。
reset	クライアントとサーバに TCP リセット メッセージを送信して、接続を終了します。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンドのモード

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
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

厳密な HTTP 検査をディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠しないトラフィックの転送をセキュリティ アプライアンスで許可することができます。このコマンドは、デフォルトの動作（HTTP に準拠しないトラフィックの転送を拒否）を上書きします。

例

次の例では、HTTP に準拠しないトラフィックの転送を許可しています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

strip-group

このコマンドが適用されるのは、user@realm の形式で受信したユーザ名のみです。レルムは、@ デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、juser@abc）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネルグループ一般アトリビュート モードで **strip-group** コマンドを使用します。セキュリティ アプライアンスは、VPN クライアントが提示するユーザ名からグループ名を取得して、PPP 接続用のトンネルグループを選択します。グループ除去処理をイネーブルにすると、セキュリティ アプライアンスは、ユーザ名のユーザ部分のみを認可と認証用に送信します。これ以外の場合（ディセーブルにした場合）、セキュリティ アプライアンスはレルムを含めてユーザ名全体を送信します。

グループ除去処理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。

strip-group

no strip-group

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、このコマンドの設定はディセーブルになっています。

コマンドのモード　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
トンネルグループ一般アトリビュート 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。

使用上のガイドライン　このアトリビュートは、IPSec リモートアクセス トンネルタイプだけに適用できます。

例

次の例では、IPSec リモートアクセス タイプ用に「remotegrp」という名前のリモートアクセス トンネルグループを設定し、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネルグループをデフォルト グループポリシーとして設定し、次にこのトンネルグループについてグループ除去をイネーブルにしています。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-group
hostname(config-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネルグループを消去します。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネルグループまたは特定のトンネルグループのトンネルグループ コンフィギュレーションを表示します。
tunnel-group-map default group	**crypto ca certificate map** コマンドを使用して作成した証明書マップ エントリを、トンネルグループに関連付けます。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネルグループ一般アトリビュート コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理は、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムを削除するものです。レルムは、@ デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、username@realm）。このコマンドをイネーブルにすると、セキュリティ アプライアンスは、ユーザ名のユーザ部分のみを認可と認証用に送信します。ディセーブルにした場合には、セキュリティ アプライアンスはユーザ名全体を送信します。

レルム除去処理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。

strip-realm

no strip-realm

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、このコマンドの設定はディセーブルになっています。

コマンドのモード

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
トンネルグループ一般アトリビュート 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。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネルタイプだけに適用できます。

例

次の例では、IPSec リモートアクセス タイプ用に「remotegrp」という名前のリモートアクセス トンネルグループを設定し、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネルグループをデフォルト グループポリシーとして設定し、次にこのトンネルグループについてレルム除去をイネーブルにしています。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-realm
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネルグループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-limit	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

subject-name (crypto ca certificate map)

規則エントリを IPSec ピア証明書のサブジェクト DN に適用することを指定するには、CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

シンタックスの説明

attr tag	証明書 DN にある、指定したアトリビュート値のみを規則エントリ文字列と比較することを指定します。タグの値を次に示します。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = 役職 O = 組織名 L = 地名 SP = 州または都道府県 C = 国または地域 OU = 組織ユニット CN = 通常名
co	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングになる必要があることを指定します。
eq	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。
nc	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングにならない必要があることを指定します。
ne	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。
string	一致するかどうかの確認対象となる値を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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 証明書マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、証明書マップ 1 の CA 証明書マップ モードに入って、証明書サブジェクト名の Organization アトリビュートが Central と等しくなる必要があると指定する規則エントリを作成しています。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。
issuer-name	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドを使用して作成した証明書マップ エントリを、トンネルグループに関連付けます。

subject-name (crypto ca trustpoint)

指定したサブジェクト DN 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 **subject-name** コマンドを使用します。これは、証明書を使用する人物またはシステムです。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。

subject-name *X.500_name*

no subject-name

シンタックスの説明

X.500_name	X.500 認定者名（たとえば、cn=crl,ou=certs,o=CAName,c=US）を定義します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルトでは、サブジェクト名を含めない設定になっています。

コマンドのモード

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、トラストポイント central 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、URL https//:frog.phoobin.com での自動登録をセットアップし、サブジェクト DN OU tiedye.com 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)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=tiedye.com
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。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment url	CA への登録用の URL を指定します。

summary-address

OSPF の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

no summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

シンタックスの説明

addr	一定範囲のアドレスに指定されたサマリー アドレスの値。
mask	サマリー ルートに使用される IP サブネット マスク。
not-advertise	（オプション）指定されたプレフィックスとマスクのペアに一致するルートを抑止します。
tag *tag_value*	（オプション）各外部ルートに付加される 32 ビットの 16 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効な値は 0 ～ 4294967295 です。

デフォルト

デフォルトは次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックスとマスクのペアに一致するルートは、抑止されません。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

他のルーティング プロトコルからラーニングしたルートは、要約することができます。このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ（ASBR）は、当該アドレスの対象となる再配布されるすべてのルートの要約として、1 つの外部ルートをアドバタイズします。このコマンドが要約するのは、他のルーティング プロトコルからラーニングした、OSPF に再配布されているルートのみです。OSPF エリア間の経路集約には、**area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を他のオプション キーワードや引数を指定せずに使用します。オプションをコンフィギュレーション内の summary コマンドから削除するには、削除するオプションを付加してこのコマンドの **no** 形式を使用します。詳細については、「例」を参照してください。

例

次の例では、***tag*** を 3 に設定して経路集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例は、デフォルト値に戻す対象オプションを指定して **summary-address** コマンドの **no** 形式を使用する方法を示しています。この例では、前の例で 3 に設定した ***tag*** の値を **summary-address** コマンドから削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例では、**summary-address** コマンドをコンフィギュレーションから削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
area range	エリアの境界でルートを統合および要約します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

sunrpc-server

SunRPC サービス テーブル内にエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリ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。

sunrpc-server *ifc_name* ***ip_addr mask*** **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **]**
timeout *hh:mm:ss*

no sunrpc-server *ifc_name* ***ip_addr mask*** **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]*
timeout *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

シンタックスの説明

ifc_name	サーバのインターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [*- port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（オプション）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC 転送プロトコルを指定します。
protocol udp	SunRPC 転送プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	タイムアウト アイドル期間を指定します。この期間を過ぎると、SunRPC サービス トラフィックへのアクセスが終了します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

SunRPC サービス テーブルは、タイムアウトで指定した期間中に、SunRPC トラフィックが確立済み SunRPC セッションに基づいてセキュリティ アプライアンスを通過することを許可するために使用します。

例

次の例は、SunRPC サービス テーブルを作成する方法を示しています。

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に認証されている場合に、リモート ユーザ証明書をそのトラストポイントに基づいて検証するには、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 **support-user-cert-validation** 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。

support-user-cert-validation

no support-user-cert-validation

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、ユーザ証明書の検証をサポートするように設定されています。

コマンドのモード

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。

使用上のガイドライン

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。このため、同じ CA から 2 つの異なる ID 証明書が発行されることがあります。あるトラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA の認証を受ける場合、このオプションは自動的にディセーブルになります。したがって、パス検証パラメータの選択であいまいさが生じることはありません。あるトラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA の認証を受けた場合は、ユーザが当該トラストポイント上でこの機能をアクティブにしようとしても、その操作は許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次の例では、トラストポイント central 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、トラストポイント central でのユーザ検証の受け入れをイネーブルにしています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
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。
default enrollment	登録パラメータをデフォルトに戻します。

syn-data

データを含んでいる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** 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。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

シンタックスの説明

allow	データを含んでいる SYN パケットを許可します。
drop	データを含んでいる SYN パケットをドロップします。

デフォルト

デフォルトでは、データを含んでいる SYN パケットは許可されます。

コマンドのモード

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
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドは、モジュラ ポリシー フレームワーク インフラストラクチャとともに使用します。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP 検査をカスタマイズします。**policy-map** コマンドを使用して新しい TCP マップを適用します。**service-policy** コマンドで TCP 検査を有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、データを含んでいる SYN パケットをドロップします。

TCP の仕様によると、TCP 実装は、SYN パケットに含まれているデータを受け入れることが要件になっています。これは仕様の微妙かつあいまいな点であり、実装の中には、このパケットを適切に処理しないものもあります。不適切なエンドシステム実装を標的にする挿入攻撃に対して、脆弱にならないようにするには、データを含んでいる SYN パケットをドロップすることをお勧めします。

例

次の例は、データを含んでいる SYN パケットをすべての TCP フローでドロップする方法を示しています。

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

関連コマンド

コマンド	説明
class（ポリシーマップ）	トラフィック分類に使用するクラスマップを指定します。
help	**policy-map**、**class（ポリシーマップ）**、および **description** コマンドのシンタックス ヘルプを表示します。
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。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

sysopt connection permit-ipsec

IPSec パケットがインターフェイスのアクセスリストをバイパスできるようにするには、グローバル コンフィギュレーション モードで **sysopt connection permit-ipsec** コマンドを使用します。グループポリシーおよびユーザごとの認可アクセスリストは、引き続きトラフィックに適用されます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection permit-ipsec

no sysopt connection permit-ipsec

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

この機能はデフォルトでイネーブルになっています。

コマンドのモード

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、デフォルトでイネーブルになりました。また、バイパスされるのはインターフェイスのアクセスリストのみです。グループポリシーおよびユーザごとのアクセスリストは有効なままです。

使用上のガイドライン

コンフィギュレーションを簡略化し、セキュリティ アプライアンスのパフォーマンスを最大限まで高めるには、IPSec トラフィックについてはインターフェイス アクセスリストをバイパスすることをお勧めします。この機能をディセーブルにする場合は、入力インターフェイスにアクセスリストを適用して、すべての IPSec ピアからの IPSec パケットを許可する必要があります（**access-list** コマンドおよび **access-group** コマンドを参照）。

例

次の例では、IPSec トラフィックがインターフェイスのアクセスリストをバイパスできるようにしています。

```
hostname(config)# sysopt connection permit-ipsec
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

TCP セグメントの最大サイズが設定した値を超えないようにし、指定したサイズよりも小さくならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** 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。

sysopt connection tcpmss [***minimum***] *bytes*

no sysopt connection tcpmss [***minimum***] [*bytes*]

シンタックスの説明

bytes	TCP セグメントの最大サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1,380 バイトです。*bytes* を 0 に設定することによって、この機能をディセーブルにできます。 ***minimum*** キーワードの場合、*bytes* は許容される最も小さい最大値を表します。
minimum	セグメントの最大サイズを上書きして、*bytes* 未満（48 ～ 65,535 バイト）にならないようにします。この機能は、デフォルトではディセーブルになっています（0 に設定されています）。

デフォルト

デフォルトの最大値は 1,380 バイトです。minimum 機能は、デフォルトではディセーブルになっています（0 に設定されています）。

コマンドのモード

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

ホストとサーバが接続を最初に確立するときは、ホストとサーバの両方でセグメントの最大サイズを設定できます。どちらかの最大サイズが **sysopt connection tcpmss** コマンドで設定した値を超えている場合、セキュリティ アプライアンスはその最大サイズを無効にして、設定した値を挿入します。どちらかの最大サイズが **sysopt connection tcpmss minimum** コマンドで設定した値よりも小さくなっている場合、セキュリティ アプライアンスはその最大サイズを無効にして、設定した「minimum」値を挿入します（minimum 値は、許容される最も小さい最大サイズです）。たとえば、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定した場合、ホストが最大サイズとして 1,300 バイトを要求しているときは、1,200 バイト（最大サイズ）を要求するようにセキュリティ アプライアンスがパケットを変更します。別のホストが最大値として 300 バイトを要求している場合、セキュリティ アプライアンスは 400 バイト（最小サイズ）を要求するようにパケットを変更します。

デフォルトの 1,380 バイトにしておくと、ヘッダー情報用の余裕ができるため、パケット全体のサイズが 1,500 バイトを超えることがなくなります。1,500 バイトは、イーサネットのデフォルト最大伝送ユニット（maximum transmission unit; MTU）です。次の計算式を参照してください。

1,380 データ + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1,500 バイト

ホストまたはサーバが最大セグメント サイズを要求しない場合、セキュリティ アプライアンスは、RFC 793 のデフォルト値である 536 バイトが有効であると想定します。

最大サイズを 1,380 バイトよりも大きい値に設定すると、MTU のサイズ（デフォルトは 1,500 バイト）によってはパケットがフラグメント化される可能性があります。フラグメントが大量に発生すると、セキュリティ アプライアンスが Frag Guard 機能を使用している場合にパフォーマンスに影響する可能性があります。最小サイズを設定しておくと、TCP サーバが小さな TCP データ パケットをクライアントに大量に送信して、サーバとネットワークのパフォーマンスに影響を与えることを防止できます。

（注） この機能を普通に使用する場合にはお勧めしませんが、syslog IPFRAG メッセージ 209001 および 209002 が発生する場合は、*bytes* 値を大きくできます。

例

次の例では、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定しています。

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が少なくとも 15 秒の短縮 TIME_WAIT 状態を保持するようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合は、この機能を使用することをお勧めします。

sysopt connection timewait

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

この機能は、デフォルトではディセーブルになっています。

コマンドのモード

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

セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後、接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスは、標準クローズ シーケンスと呼ばれる一般的なクロージング シーケンスに基づいて、高接続率を保つことができます。ただし、一方のエンドがクローズし、もう一方のエンドは確認応答してからクロージング シーケンスを開始する標準クローズ シーケンスとは対照的に、同時クローズでは、トランザクションの両エンドがクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放により、接続の 1 つのサイドで CLOSING 状態が保持されます。CLOSING 状態の多くのソケットがある場合は、エンド ホストのパフォーマンスが低下することがあります。たとえば、一部の WinSock メインフレーム クライアントは、このような動作を示し、メインフレーム サーバのパフォーマンスを低下させることが確認されています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスを完了するためのウィンドウが作成されます。

例

次の例では、timewait（一時停止）機能をイネーブルにしています。

```
hostname(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。

sysopt nodnsalias

alias コマンドを使用する場合に、DNS の A レコード アドレスを変更する DNS 検査をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt nodnsalias** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**alias** コマンドで NAT のみを実行して、DNS パケットの変更が不要な場合には、DNS アプリケーション検査をディセーブルにすることをお勧めします。

sysopt nodnsalias {***inbound*** | ***outbound***}

no sysopt nodnsalias {***inbound*** | ***outbound***}

シンタックスの説明

inbound	セキュリティの低いインターフェイスから、**alias** コマンドで指定したセキュリティの高いインターフェイスに向かうパケットの DNS レコード変更をディセーブルにします。
outbound	**alias** コマンドで指定した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に向かうパケットの DNS レコード変更をディセーブルにします。

デフォルト

この機能は、デフォルトではディセーブルになっています。つまり、DNS レコードのアドレス変更がイネーブルになっています。

コマンドのモード

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

alias コマンドは、NAT、および DNS の A レコードのアドレス変更を実行します。DNS レコードの変更は、特定の状況下ではディセーブルにしたほうがよい場合もあります。

例

次の例では、着信パケットについて DNS アドレスの変更をディセーブルにしています。

```
hostname(config)# sysopt nodnsalias inbound
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt noproxyarp	インターフェイス上でのプロキシ ARP をディセーブルにします。

sysopt noproxyarp

NAT グローバル アドレスに対するインターフェイス上でのプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。グローバル アドレスに対するプロキシ ARP を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

シンタックスの説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

デフォルトでは、グローバル アドレスに対するプロキシ ARP はイネーブルになっています。

コマンドのモード

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

まれに、グローバル アドレスに対するプロキシ ARP をディセーブルにしたほうがよい場合もあります。

ホストが IP トラフィックを同じイーサネット ネットワーク上の別のデバイスに送信するとき、ホストはデバイスの MAC アドレスを知っている必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスは誰なのか」という ARP 要求を送信します。当該の IP アドレスを所有しているデバイスは、「その IP アドレスを所有している。これが私の MAC アドレスだ」という応答を返します。

プロキシ ARP は、デバイスが当該の IP アドレスを所有していない場合でも、デバイスが自身の MAC アドレスで ARP 要求に応答する動作です。NAT を設定して、セキュリティ アプライアンス インターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、セキュリティ アプライアンスはプロキシ ARP を使用します。トラフィックがホストに到達する唯一の方法は、セキュリティ アプライアンスがプロキシ ARP を使用して、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次の例では、内部インターフェイス上でのプロキシ ARP をディセーブルにしています。

```
hostname(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答に含まれている認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。一部の RADIUS サーバとの互換性を維持するには、このキーを無視する必要があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

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

この機能は、デフォルトではディセーブルになっています。

コマンドのモード

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

Livingston Version 1.16 など、一部の RADIUS サーバでは、アカウンティング確認応答の認証ハッシュ内にキーが含まれていないという使用上の注意点があります。このような場合、セキュリティ アプライアンスがアカウンティング要求を継続的に再送信することがあります。**sysopt radius ignore-secret** コマンドは、アカウンティング確認応答の認証キーを無視して、再送信の問題を回避するために使用します。ここで説明しているキーとは、**aaa-server host** コマンドで設定するキーです。

例

次の例では、アカウンティング応答に含まれている認証キーを無視しています。

```
hostname(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。

sysopt uauth allow-http-cache

Web ブラウザがセキュリティ アプライアンス上の仮想 HTTP サーバ（**virtual http** コマンドを参照）から再認証を受ける場合に、キャッシュにあるユーザ名とパスワードを Web ブラウザが使用できるようにするには、グローバル コンフィギュレーション モードで **sysopt uauth allow-http cache** コマンドを使用します。HTTP キャッシュを許可しない場合は、認証セッションがタイムアウトすると、次に仮想 HTTP サーバに接続したときにユーザ名とパスワードの再入力を求められます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt uauth allow-http-cache

no sysopt uauth allow-http-cache

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

この機能は、デフォルトではディセーブルになっています。

コマンドのモード

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。

例

次の例では、HTTP キャッシュの使用を許可しています。

```
hostname(config)# sysopt uauth allow-http-cache
```

関連コマンド

コマンド	説明
virtual http	セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求している場合、このコマンドを使用すると、セキュリティ アプライアンスと HTTP サーバで別々に認証を実行できます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。