CHAPTER 30

show service-policy ～ show xlate コマンド

show service-policy

設定されたサービス 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 ***service-policy*** コマンドを使用します。

show service-policy [**global** | ***interface*** *intf*] [***action*** | ***flow*** *flow_descriptor*] [***priority***]

シンタックスの説明

policymap_name	英数字で表された一意のポリシー マップ ID
global	すべてのインターフェイスに対するポリシー マップを表示します。
interface	特定のインターフェイスに対するポリシー マップを表示します。
intf	***nameif*** コマンドで定義されたインターフェイス名
action	統計情報または動作データを表示するアクションを指定します。
priority	インターフェイス ポリシー マップのトラフィック カウント プライオリティを表示します。
flow	設定されたポリシーを表示するデータ フローを指定します。***flow*** キーワードの構文および適切な使用法については、「使用上のガイドライン」を参照してください。 • ***protocol*** — データ フローで使用されるプロトコル • ***host source_ip*** | ***source_ip*** *source_mask* — データ フローで使用されるホスト送信元 IP、または送信元 IP アドレスおよび送信元ネットマスク • ***source_ip*** — データ フローで使用される送信元 IP アドレス • *source_mask* — データ フローで使用される送信元 IP ネットマスク • ***eq*** — 指定されたポートと同じポート番号を一致させる演算子 • ***source_port*** — データ フローで使用される送信元ポート • ***destination_ip*** — データ フローで使用される宛先 IP アドレス • *destination_mask* — データ フローで使用される宛先 IP アドレスのサブネット マスク • ***destination_port*** — データ フローで使用される宛先ポート • ***icmp*** — データ フローで ICMP トラフィックを使用するように指定します。 • *icmp_type* — データ フローで使用される ICMP トラフィックのタイプを指定します。

flow_descriptor	フローを示す一意の名前

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

設定されたポリシーを表示するデータ フローを指定するには、***flow*** キーワードを使用します。*flow_descriptor* は、ip-5-tuple 形式です。オブジェクトはグループ化されません。

protocol [***host source_ip*** | ***source_ip*** *source_mask*] [***eq*** *source_port*]

[***host destination_ip*** | ***destination_ip*** *destination_source*] [***eq*** *destination_port*]

icmp [***host source_ip*** | ***source_ip*** *source_mask*]

{***host destination_ip*** | ***destination_ip*** *destination_mask*] [*icmp_type*]

フローは ip-5-tuple 形式であるため、一致基準の一部はサポートされません。次に、フロー照合でサポートされている一致基準を示します。

- ***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介して送信されるパケットの合計カウンタ値を表示する場合に使用します。

show service-policy コマンド出力に表示される初期接続数は、**class-map** コマンドで定義された、トラフィック マッチングに使用される、インターフェイスとの現在の初期接続数を示します。`embryonic-conn-max` フィールドには、Modular Policy Framework を使用するトラフィック クラスに設定された最大初期制限が表示されます。表示されている現在の初期接続数が最大値と同じか、または最大値を超えている場合、**class-map** コマンドで定義されたトラフィック タイプと一致する新しい TCP 接続には、TCP 代行受信が適用されます。

例

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

```
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 ポリシー設定を消去します。
clear service-policy	サービス ポリシー設定をすべて消去します。
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で設定されたサービス ポリシーを表示します。

show service-policy inspect gtp

GTP 設定を表示するには、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	（任意）指定された APN に基づいて Packet Data Protocol（PDP）コンテキストの詳細出力を表示します。
ap_name	統計情報を表示する特定のアクセス ポイント名を識別します。
detail	（任意）PDP コンテキストの詳細出力を表示します。
imsi	指定された IMSI に基づいて PDP コンテキストの詳細出力を表示します。
IMSI_value	統計情報を表示する特定の IMSI を識別する 16 進数
interface	（任意）特定のインターフェイスを識別します。
int	情報を表示するインターフェイスを識別します。
gsn	（任意）GPRS 無線データ ネットワークとその他のネットワーク間のインターフェイスとなる GPRS サポート ノードを識別します。
gtp	（任意）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	（任意）指定された Mobile Station（MS）アドレスに基づいて PDP コンテキストの詳細出力を表示します。
pdp-context	（任意）PDP コンテキストを識別します。
pdpmcb	（任意）PDP マスター制御ブロックのステータスを表示します。
requests	（任意）GTP 要求のステータスを表示します。
statistics	（任意）GTP の統計情報を表示します。
tid	（任意）指定された TID に基づいて PDP コンテキストの詳細出力を表示します。
tunnel_ID	統計情報を表示する特定のトンネルを識別する 16 進数
version	（任意）GTP バージョンに基づいて PDP コンテキストの詳細出力を表示します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

縦棒（|）を使用して、出力をフィルタリングできます。| を入力して、複数のフィルタリング オプションで出力することもできます。

show pdp-context コマンドは、PDP コンテキスト関連情報を表示します。

PDP コンテキストは、IMSI および NSAPI を組み合わせたトンネル ID で識別されます。GTP トンネルは異なる GSN ノード内にある 2 つの対応する PDP コンテキストによって定義され、トンネル ID で識別されます。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 ユーザ間でパケットを転送する場合は、GTP トンネルが必要です。

show gtp requests コマンドは、要求キュー内の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、縦棒（|）を使用して、出力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 という文字列を含む GTP 統計情報が表示されます。

次のコマンドは、GTP 検査に関する統計情報を示します。

```
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
```

次のコマンドは、PDP コンテキストに関する情報を表示します。

```
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 30-1 に、**show service-policy inspect gtp pdp-context** コマンド出力内の各カラムの説明を示します。

表 30-1　PDP コンテキスト

カラム見出し	説明
Version	GTP のバージョン
TID	トンネル ID
MS Addr	モバイル ステーションのアドレス
SGSN Addr	処理中のゲートウェイ サービス ノード
Idle	PDP コンテキストが使用されなかった時間
APN	アクセス ポイント名

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査の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	特定の GTP マップがアプリケーション検査で使用されるようにします。

show shun

遮断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	（任意）該当するアドレスの情報を表示します。
statistics	（任意）インターフェイス カウンタのみを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、**show 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	現在イネーブル化されている遮断をすべてディセーブルにし、遮断に関する統計情報を消去します。
shun	新しい接続や既存の接続からのパケットを禁止して、攻撃元ホストへのダイナミック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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show sip コマンドは SIP インスペクション エンジンに関する問題のトラブルシューティングに役立ちます。説明については、**inspect protocol sip udp 5060** コマンドを参照してください。**show timeout sip** コマンドは、指定された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、FWSM に確立された SIP セッションの情報を表示します。このコマンドと **debug sip** および **show local-host** コマンドを組み合わせて、SIP インスペクション エンジンの問題に関するトラブルシューティングを行うことができます。

（注）　**pager** コマンドを設定してから、**show sip** コマンドを使用することを推奨します。多数の SIP セッション レコードが存在する場合に **pager** コマンドが設定されていないと、**show sip** コマンド出力が終了するまでに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
```

この例では、FWSM の 2 つのアクティブな SIP セッションを示しています（`Total` フィールドに表示されます）。各 `call-id` はコールを表します。

最初のセッション（`call-id c3943000-960ca-2e43-228f@10.130.56.44`）は `Call Init` 状態にあり、セッションはコール セットアップ中です。コール セットアップが完了すると、ACK が表示されます。このセッションは 1 秒間アイドルでした。

2 番めのセッションは Active 状態です。コール セットアップは完了していて、エンドポイントがメディアを交換中です。このセッションは 6 秒間アイドルでした。

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	各接続タイプの接続状態を表示します。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

show skinny

SCCP（Skinny）インスペクション エンジンに関する問題のトラブルシューティングを行うには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny [**audio** | **video**]

シンタックスの説明

audio	出力を音声関連情報に限定します。
video	出力をビデオ関連情報に限定します。

デフォルト

audio または **video** キーワードを使用しない場合、出力には音声とビデオの両方の情報が必要に応じて含まれます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show skinny コマンドは SCCP（Skinny）インスペクション エンジンに関する問題のトラブルシューティングに役立ちます。

例

次に、以下の条件における **show skinny** コマンドの出力例を示します。FWSM にアクティブな Skinny セッションが 2 つ設定されています。最初のセッションは、ローカル アドレスが 10.0.0.11 の内部 Cisco IP Phone と 172.18.1.33 の外部 Cisco CallManager の間に確立された音声セッションです。TCP ポート 2000 は CallManager です。2 番めのセッションは、ローカル アドレスが 10.0.0.22 の別の内部 Cisco IP Phone と、同じ Cisco CallManager の間に確立されたビデオ セッションです。

```
hostname# show skinny
LOCAL                    FOREIGN                  STATE
--------------------------------------------------------------------
1       10.0.0.11/52238          172.18.1.33/2000                1
  AUDIO 10.0.0.11/22948          172.18.1.22/20798
2       10.0.0.22/52232          172.18.1.33/2000                1
  VIDEO 10.0.0.22/20798          172.18.1.11/22948
```

出力は、両方の内部 Cisco IP Phone 間にコールが確立されたことを示します。最初および 2 番めの Phone の RTP 待ち受けポートは、それぞれ UDP 22948 および 20798 です。

次に、これらの Skinny 接続の 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
```

video キーワードを使用した場合、出力は次の例のようにビデオ セッション情報に限定されます。

```
hostname# show skinny video
LOCAL                    FOREIGN                  STATE
--------------------------------------------------------------------
1       10.0.0.22/52232          172.18.1.33/2000                1
  VIDEO 10.0.0.22/20798          172.18.1.11/22948
```

audio キーワードを使用した場合、出力は次の例のように音声セッション情報に限定されます。

```
hostname# show skinny audio
LOCAL                    FOREIGN                  STATE
--------------------------------------------------------------------
1       10.0.0.11/52238          172.18.1.33/2000                1
  AUDIO 10.0.0.11/22948          172.18.1.22/20798
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug skinny	SCCP 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	各接続タイプの接続状態を表示します。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

show snmp-server statistics

SNMP（簡易ネットワーク管理プロトコル）サーバの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、引数またはキーワードはありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

例

次に、SNMP サーバの統計情報を表示する例を示します。

```
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 イベント情報を提供します。
clear configure snmp-server	SNMP サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバ設定を表示します。

show ssh sessions

FWSM のアクティブな SSH 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 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	（任意）指定された IP アドレスのみのセッション情報を表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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の番号です。Client IP は SSH クライアントで稼働するシステムの IP アドレスです。Version は、SSH クライアントがサポートするプロトコル バージョン番号です。SSH クライアントが SSH Version 1 のみをサポートする場合、Version カラムには 1.5 が表示されます。SSH クライアントが SSH Version 1 および SSH Version 2 をサポートする場合、Version カラムには 1.99 が表示されます。SSH クライアントが SSH Version 2 のみをサポートする場合、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タイプが表示されます。State カラムには、FWSM と交信しているときのクライアントの進行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たログイン 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	アイドルな 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したり、スタートアップ コンフィギュレーションをロードするときに発生したエラーを表示するには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [errors]

シンタックスの説明

errors	（任意）FWSM がスタートアップ コンフィギュレーションをロードするときに生成されたエラーを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム[1]
特権 EXEC	•	•	•	•	•

1. **errors** キーワードを使用できるのは、シングル モードおよびシステム実行スペースのみです。

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
3.1(1)	**errors** キーワードが追加されました。

使用上のガイドライン

マルチ コンテキスト モードの場合、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。

メモリから起動時のエラーを消去するには、**clear startup-config errors** コマンドを使用します。

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
```

次に、**show startup-config errors** コマンドの出力例を示します。

```
hostname# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "  limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', " nameif inside"
.....
*** Output from config line 37, "  config-url disk:/admin..."
```

関連コマンド

コマンド	説明
clear startup-config errors	メモリから起動時のエラーを消去します。
show running-config	実行コンフィギュレーションを表示します。

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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

Sun RPC サービス（NFS や NIS）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** コマンドを使用します。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	FWSM から Sun RPC サービスを消去します。
clear sunrpc-server active	Sun RPC サービス（NFS や NIS など）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、使用するポートを設定します。
show running-config sunrpc-server	Sun RPC サービスの設定に関する情報を表示します。

show tcpstat

FWSM TCP スタックおよび FWSM で終端する 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 および IPv6 アドレスをサポートします。

show tcpstat

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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 FWSM で終端する TCP 接続のステータスを表示できます。表 30-2 に、表示される TCP 統計情報を示します。

表 30-2　show tcpstat コマンドで表示される TCP 統計情報

統計情報	説明
tcb_cnt	TCP ユーザ数
proxy_cnt	TCP プロキシ数。TCP プロキシはユーザ許可で使用されます。
tcp_xmt pkts	TCP スタックで送信されたパケット数
tcp_rcv good pkts	TCP スタックで受信された良好なパケット数
tcp_rcv drop pkts	TCP スタックが廃棄した受信パケット数
tcp bad chksum	チェックサムが不正な受信パケット数
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザ数
tcp user hash add dup	追加しようとした新規 TCP ユーザがハッシュ テーブルに格納済みであった回数
tcp user srch hash hit	検索した TCP ユーザがハッシュ テーブルに格納されていた回数
tcp user srch hash miss	検索した TCP ユーザがハッシュ テーブルに格納されていなかった回数
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	削除しようとした TCP ユーザがハッシュ テーブルに格納されていなかった回数
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

表 30-2　show tcpstat コマンドで表示される TCP 統計情報（続き）

統計情報	説明
fp	TCP ユーザの外部ポート
st	TCP ユーザの状態（RFC 793 を参照）。有効値は、次のとおりです。 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 ユーザの非アクティブ タイムアウト タイマーの値（ミリ秒）
cl_timer	TCP ユーザの終了要求タイマーの値（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 ユーザの再送信回数

例

次に、**show tcpstat** コマンドの出力例を示します。

```
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および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	（任意）詳細を表示します。
file	（任意）コマンド出力をファイルに書き込みます。
no-config	（任意）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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	***detail*** および ***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 コマンドを使用すると、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必要な情報を表示できます。このコマンドは、テクニカル サポート アナリストに必要なほとんどの情報を提供するいくつかの **show** コマンドの出力を統合します。

例

次に、テクニカル サポート アナリストが使用する情報を、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例を示します。

```
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）および Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）プロトコルで使用するクロックを表示します。
show conn count	使用されている接続および使用可能な接続を表示します。
show cpu	CPU 利用率情報を表示します。
show failover	接続のステータスおよびアクティブな FWSM を表示します。
show memory	OS（オペレーティング システム）で使用可能な最大物理メモリおよび現在の空きメモリに関するサマリーを表示します。
show perfmon	FWSM のパフォーマンスに関する情報を表示します。
show processes	稼働しているプロセスのリストを表示します。
show running-config	FWSM の現在の実行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 time-range

時間範囲エントリを表示するには、特権 EXEC モードで **show time-range** コマンドを使用します。

show time-range [*time-range*]

シンタックスの説明

time-range	（任意）時間範囲エントリの名前。

デフォルト

デフォルトでは、すべての時間範囲エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

この例では、**show time-range** を使用してすべての時間範囲エントリを表示しています。

```
hostname(config)# show time-range
time-range entry: test (inactive)
absolute start 11:03 14 April 2006 end 11:06 14 April 2006
```

関連コマンド

コマンド	説明
clear configure time-range	設定された時間範囲を消去します。
show running-config time-range	設定されたすべての時間範囲を表示します。

show traffic

インターフェイスの送受信アクティビティ、およびコントロール プレーンを通過するトラフィックを表示するには、特権 EXEC モードで ***show traffic*** コマンドを使用します。コントロール プレーン パスを通過するパケットには、レイヤ 7 検査を必要とするプロトコルのための制御パケットや、管理トラフィックなどがあります。

show traffic [**detailed** [*type*] | **summary** [*type*]]

シンタックスの説明

detailed	（任意）コントロール プレーンの詳細なトラフィック カウンタを表示します。
summary	（任意）コントロール プレーンのトラフィック サマリー カウンタを表示します。
type	（任意）特定のトラフィック タイプのカウンタを表示します。トラフィック タイプ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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
3.1(1)	**summary** および **detailed** キーワードが追加されました。

使用上のガイドライン

show traffic コマンド（キーワードを指定しない場合）は、最後に **show traffic** コマンドを入力してから、または FWSM がオンラインになってから、各インターフェイスを通過したパケット数およびバイト数を表示します。表示される秒数は、最後に再起動してから FWSM がオンラインになっている期間を示します。ただし、最後に再起動したあとに **clear traffic** コマンドを入力した場合、表示される秒数はコマンドを入力したあとの期間を示します。

summary および **detailed** キーワードを指定した場合は、コントロール プレーンを通過したトラフィックがパケット タイプ別に表示されます。

マルチ モードの場合は、すべてのコンテキストの累積値、およびコンテキストごとのカウンタが表示されます。

表 30-3 に、トラフィック タイプを示します。

表 30-3　トラフィック タイプ

タイプ	説明
activex	ActiveX フィルタリング
all	検査するすべてのトランスポート プロトコルのカウンタを表示
ctiqbe	CTIQBE プロトコル

表 30-3　トラフィック タイプ

タイプ	説明
dns	UDP ベースのドメイン ネーム サービス
domain	TCP ベースのドメイン ネーム サービス
ftp	FTP
ftp-filter	FTP コマンド フィルタリング
gtp	GTP プロトコル
h323-h225	H225 プロトコル
h323-ras	H225 ras プロトコル
http	HTTP
https-filter	HTTPS プロトコル フィルタリング
ils	ILS プロトコル
java	Java フィルタリング
mgcp	MGCP プロトコル
netbios	NetBIOS プロトコル
pptp	PPTP
rpc	TCP RPC プロトコル
rpc-udp	UDP ベース RPC プロトコル
rsh	リモート シェル
rtsp	Real Time Streaming Protocol
sftp	Strict FTP
sip	TCP ベース SIP プロトコル
skinny	Skinny プロトコル
smtp	SMTP プロトコル
snmp	SNMP プロトコル
sqlnet	SQLNet プロトコル
sunrpc	TCP ベース SunRPC プロトコル
sunrpc-udp	UDP ベース SunRPC プロトコル
tftp	TFTP
udp-sip	UDP ベース SIP プロトコル
url-filter	URL フィルタリング
xdmcp	XDMCP プロトコル

例

次に、**show traffic** コマンドの出力例を示します。

```
hostname# show traffic
inside:
        received (in 1557469.650 secs):
                157532 packets  13588525 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 1557469.650 secs):
                157496 packets  13929928 bytes
                0 pkts/sec      0 bytes/sec
```

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

```
hostname# show traffic summary

--------------------------------------------------------------------------------
  Traffic Type     Pkts-In      Bytes-In   Conn-Created    Conn-Destroyed
--------------------------------------------------------------------------------
   url-filter            0             0              0                 0
          dns            0             0              0                 0
      activex            0             0              0                 0
         java            0             0              0                 0
       domain            0             0              0                 0
          sftp           0             0              0                 0
           ftp           0             0              0                 0
          http           0             0              0                 0
    h323-h225            0             0              0                 0
     h323-ras            0             0              0                 0
          ils            0             0              0                 0
       sunrpc            0             0              0                 0
          rpc            0             0              0                 0
          rsh            0             0              0                 0
         rtsp            0             0              0                 0
         smtp            0             0              0                 0
       sqlnet            0             0              0                 0
          sip            0             0              0                 0
       skinny            0             0              0                 0
   sunrpc-udp            0             0              0                 0
      rpc-udp            0             0              0                 0
        xdmcp            0             0              0                 0
      udp-sip            0             0              0                 0
      netbios            0             0              0                 0
       ctiqbe            0             0              0                 0
   ftp-filter            0             0              0                 0
 https-filter            0             0              0                 0
         mgcp            0             0              0                 0
         tftp            0             0              0                 0
         snmp            0             0              0                 0
         pptp            0             0              0                 0
          gtp            0             0              0                 0

--------------------------------------------------------------------------------
```

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

```
hostname# show traffic detailed

Traffic Class: url-filter
                                    packets received              0
                                      bytes received              0
                                  connections created             0
                                connections destroyed             0
                           delete indications received            0
    garbage collection initiated connection closure               0
     connections destroyed due to flow handle reuse               0
                     control channel create requests              0
                        data channel create requests              0
Traffic Class: dns
                                    packets received              0
                                      bytes received              0
                                  connections created             0
                                connections destroyed             0
                           delete indications received            0
    garbage collection initiated connection closure               0
     connections destroyed due to flow handle reuse               0
   connections closure initiated from control plane               0
                     control channel create requests              0
                        data channel create requests              0
....
```

関連コマンド

コマンド	説明
clear traffic	送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特定のユーザ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、およびキャッシュされた IP およびポート許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	（任意）表示するユーザ認証および許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、すべてのユーザの許可情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

show uauth コマンドは特定のユーザまたはすべてのユーザの AAA（認証、認可、アカウンティング）許可および認証キャッシュを表示します。

このコマンドは、**timeout** コマンドと併せて使用します。

各ユーザ ホストの IP アドレスには、許可キャッシュがアタッチされます。キャッシュでは、ユーザ ホストごとに最大 16 のアドレスおよびサービスのペアを使用できます。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、FWSM はユーザを許可済みであるとみなし、すぐに接続を代行処理します。たとえば、ある Web サイトへのアクセスを一度許可すると、イメージを読み込むたびに許可サーバと通信することがなくなります（イメージが同じ IP アドレスから読み込まれる場合）。これにより、許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、認証および許可の目的で許可サーバに提供されたユーザ名、およびユーザ名がバインドされている IP アドレスが表示されます。また、ユーザが認証されただけであるか、それともキャッシュされたサービスを持っているのかも表示されます。

（注）　Xauth をイネーブルにすると、uauth テーブル（**show uauth** コマンドで表示）に、クライアントに割り当てられた IP アドレスに関するエントリが追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用する場合、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背後のユーザを単一の 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 許可またはアカウンティング サービスが必要な場合は、AAA 認証プロキシをイネーブルにして、ファイアウォール背後のユーザを認証できます。AAA 認証プロキシの詳細については、**aaa** コマンドを参照してください。

ユーザ接続がアイドルになったあと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許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は、再認証する必要が生じます。

例

次に、認証されたユーザがいない状態で、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、かつ FWSM を介してサービスを使用することが許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	現在のユーザ認証および許可情報を削除します。
timeout	最大アイドル期間を設定します。

show url-block

URL ブロック バッファ内のパケット数、およびバッファ制限または再送信回数を超過したために廃棄されたパケット数（存在する場合）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	（任意）ブロック バッファ使用率に関する統計情報を表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

show url-block block statistics コマンドは、URL ブロック バッファ内のパケット数、およびバッファ制限または再送信回数を超過したために廃棄されたパケット数（存在する場合）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
```

このコマンドを実行すると、URL ブロック バッファの設定が表示されます。

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 バッファ使用率カウンタを消去します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
url-block	Web サーバ応答に使用される URL バッファを管理します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

show url-cache statistics

N2H2 または Websense フィルタリング サーバからの応答を待機する間 URL をバッファに格納するための URL キャッシュの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、引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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 — **url-cache** *size* オプションで設定されるキャッシュ サイズ（キロバイト）
- Entries — キャッシュ サイズに基づく最大キャッシュ エントリ数
- In Use — キャッシュ内の現在のエントリ数
- Lookups — FWSM がキャッシュ エントリを検索した回数
- Hits — FWSM がキャッシュ内にエントリを検出した回数

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するには、**show perfmon** コマンドを使用します。

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** コマンドのステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに転送します。
url-block	Web サーバ応答に使用される URL バッファを管理します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

show url-server

URL フィルタリング サーバの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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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 数（総数、許可、拒否）、HTTPS 接続数（総数、許可、拒否）、TCP 接続数（総数、許可、拒否）、および URL サーバの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 の場合は、**url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- Websense の場合は、**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 サーバに転送します。
url-block	Web サーバ応答に使用される URL バッファを管理します。
url-cache	N2H2 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 サイズを設定します。
url-server	**filter** コマンドで使用する N2H2 または Websense サーバを識別します。

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、ユーザ 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、引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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、最後に再起動してからの動作時間、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 キーの値、ライセンス タイプ（R または UR）、および設定を前回変更したときのタイム スタンプを表示できます。

show version コマンドによって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 の番号です。この番号は、シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを入手した場合は、シャーシの番号でなく、**show version** コマンドで表示されるシリアル番号が必要になります。

（注）　稼働時間の値はフェールオーバー セットの稼働時間を示します。特定の装置が動作を停止しても、他の装置が動作を継続しているかぎり、稼働時間の値は増加し続けます。

例

次に、Cisco PIX 500 シリーズ FWSM のソフトウェア 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の情報を表示する例を示します。

```
hostname> show version
Cisco PIX Firewall Version 7.0(1)
PIX (7.0.1.0) #15: Tue XXX 17 14:03:28 EDT 2005
pixfirewall up 5 days 21 hours
Hardware: PIX-515, 96 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash unknown @ 0x0, 0KB
0: Ext: Ethernet0 : media index 0: irq 10
1: Ext: Ethernet1 : media index 1: irq 7
License Features for this Platform:
Maximum Physical Interfaces : 3
Maximum VLANs : 10
Inside Hosts : Unlimited
Failover : Disabled
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Failover standby only : Disabled
Cut-through Proxy : Enabled
Guards : Enabled
URL-filtering : Enabled
Security Contexts : 0
GTP/GPRS : Disabled
VPN Peers : Unlimited
This machine has a Restricted (R) license.
Serial Number: 12345678
Running Activation Key: 0xbd27f269 0xbc7ebd46 0x1c73e474 0xbb782818 0x071dd0a6
```

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	FWSM の稼働時間を表示します。

show vlan

システム VLAN（仮想 LAN）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 vlan** コマンドを使用します。

show vlan

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

show vlan コマンドを使用すると、スイッチに追加された VLAN のみが表示されます。

例

次に、システム VLAN を表示する例を示します。

```
hostname(config)# show vlan
10-11, 30, 40, 300
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
clear vlan	VLAN を削除します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスのランタイム ステータスおよび統計情報を表示します。

show vpn-sessiondb

VPN（バーチャル プライベート ネットワーク）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、情報を完全に、または詳細に表示するためのオプションがあります。表示するセッション タイプを指定し、情報をフィルタリングしたり並べ替えるためのオプションを指定してください。構文の表および「使用上のガイドライン」に、選択できるオプションがまとめられています。

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

表示精度	
detail	セッションの詳細を表示します。たとえば、IPSec セッションに **detail** オプションを使用すると、IKE ハッシング アルゴリズム、認証モード、鍵再設定インターバルなどの詳細が表示されます。 **detail** および **full** オプションを選択すると、詳細出力は機械が読み取り可能な形式で表示されます。
filter	1 つまたは複数のフィルタ オプションを使用して指定された情報のみが表示されるように、出力をフィルタリングします。詳細については、使用上のガイドラインを参照してください。
full	送信された、切り捨てられていない出力を表示します。出力は | 文字で区切られ、レコード間には || 文字列が挿入されます。
sort	指定された並べ替えオプションに従って、出力を並べ替えます。詳細については、使用上のガイドラインを参照してください。
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。この情報は、特定の電子メール プロキシ セッションについて表示したり、**name**（接続名）、**ipaddress**（クライアント）**encryption** のフィルタ オプションおよび並べ替えオプションを使用してフィルタリングすることができます。
index indexnumber	インデックス番号を基準として、単一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 オプションおよび並べ替え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。この情報は、すべてのグループについて表示したり、**name**、**ipaddress**、**protocol**、**encryption** のフィルタ オプションや並べ替えオプションを使用してフィルタリングすることができます。
remote	リモートアクセス セッションを表示します。この情報は、すべてのグループについて表示したり、**name**、**a-ipaddress**、**p-ipaddress**、**tunnel-group**、**protocol**、**encryption** のフィルタ オプションを使用してフィルタリングすることができます。
webvpn	WebVPN セッションに関する情報を表示します。この情報は、すべてのグループについて表示したり、**name**、**ipaddress**、**encryption** のフィルタ オプションや並べ替えオプションを使用してフィルタリングすることができます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン　次のオプションを使用して、セッション出力をフィルタリングしたり、並べ替えることができます。

フィルタ / 並べ替えオプション	意味
filter a-ipaddress *IPaddr*	割り当てられた特定の IP アドレス（複数可）の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。
sort a-ipaddress	割り当てられた IP アドレスを基準に、出力を並べ替えます。
filter encryption *encryption-algo*	指定された暗号化アルゴリズムを使用するセッション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。
sort encryption	暗号化アルゴリズムを基準に、出力を並べ替えます。 暗号化アルゴリズムは次のとおりです。 aes128　des aes192　3des aes256　rc4
filter ipadddress *IPaddr*	指定された内部 IP アドレス（複数可）の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。
sort ipaddress	内部 IP アドレスを基準に、出力を並べ替えます。
filter name *username*	指定されたユーザ名に対応するセッションを表示するように、出力をフィルタリングします。
sort name	ユーザ名のアルファベット順に、出力を並べ替えます。
filter p-address *IPaddr*	指定された外部 IP アドレスの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。
sort p-address	指定された外部 IP アドレス（複数可）を基準に、出力を並べ替えます。
filter protocol *protocol-name*	指定されたプロトコル（複数可）を使用するセッション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。

フィルタ / 並べ替えオプション	意味
sort protocol	プロトコルを基準に、出力を並べ替えます。 プロトコルは、次のとおりです。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
filter tunnel-group *groupname*	指定されたトンネル グループ（複数可）の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。
sort tunnel-group	トンネル グループを基準に、出力を並べ替えます。
| character	出力を変更します。使用される引数は、{begin | include | exclude | grep | [-v]} {reg_exp} です。
<cr>	出力をコンソールに送信します。

次に、特権 EXEC モードでコマンドを入力し、LAN-to-LAN セッションの詳細情報を表示する例を示します。

```
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 セッションのサマリーを表示します。

show vpn-sessiondb ratio

プロトコルまたは暗号化アルゴリズムを基準として、現在のセッションの比率をパーセントで表示するには、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識別します。フェーズ 2 暗号化を意味します。暗号化アルゴリズムは次のとおりです。 aes128　des aes192　3des aes256　rc4
filter *groupname*	指定されたトンネル グループのセッション比率のみを表示するように、出力をフィルタリングします。
protocol	表示するプロトコルを識別します。プロトコルは、次のとおりです。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

例

次に、**show vpn-sessiondb ratio** コマンドに **encryption** 引数を指定した場合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、**show vpn-sessiondb ratio** コマンドに **protocol** 引数を指定した場合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%
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	詳細を含めて、あるいは含めないで、セッションを表示します。指定した基準に従ってセッションをフィルタリングしたり、並べ替えることもできます。
show vpn-sessiondb summary	現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。

show vpn-sessiondb summary

現在の VPN（バーチャル プライベート ネットワーク）セッションのサマリーを表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。

show vpn-sessiondb summary

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

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	詳細を含めて、あるいは含めないで、セッションを表示します。指定した基準に従ってセッションをフィルタリングしたり、並べ替えることもできます。
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	変換数を表示します。
debug	（任意）xlate デバッグ情報を表示します。
detail	（任意）xlate の詳細情報を表示します。
global *ip1*[**-***ip2*]	（任意）アクティブな変換をグローバル IP アドレス別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 ポート別またはポート範囲別に表示します。
interface *if_name*	（任意）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*]	（任意）アクティブな変換をローカル IP アドレス別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 ポート別またはポート範囲別に表示します。
netmask *mask*	（任意）グローバルまたはローカル IP アドレスを修飾するネットワーク マスクを指定します。
state *state*	（任意）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（ポート アドレス変換）グローバル変換を指定します。 • ***norandomseq*** **—** ***norondomseq*** 設定を使用した **nat** または **static** 変換を指定します。 • ***identity*** **— nat 0** ID 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、スペースで区切ります。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

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 30-4 に変換フラグの定義を示します。

表 30-4　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 ARR 再書き込み
I	**nat 0** からの ID 変換

（注） **vpnclient** 設定がイネーブルで、内部ホストが DNS 要求を送信している場合に、**show xlate** コマンドを実行すると、1 つのスタティック変換に対応する 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。3 つの PAT がアクティブである場合の変換スロット情報が表示されます。

```
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。3 つの PAT がアクティブである場合の変換タイプおよびインターフェイス情報が表示されます。

最初のエントリは、内部ネットワークのホスト ポート（10.1.1.15、1025）から外部ネットワークのホスト 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ます。

2 番めのエントリは、内部ネットワークのホスト ポート（10.1.1.15、1028）から外部ネットワークのホスト 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ます。

3 番めのエントリは、内部ネットワークのホスト ICMP ID（10.1.1.15、21505）から外部ネットワークのホスト ICMP ID（192.150.49.1、0）への ICMP PAT です。r フラグは、変換が PAT であることを示します。i フラグは、変換が内部 ICMP ID に適用されることを示します。

セキュリティが高いインターフェイスから低いインターフェイスに移動するパケットの場合、内部アドレス フィールドは送信元アドレスとして表示されます。セキュリティが低いインターフェイスから高いインターフェイスに移動するパケットでは、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。スタティック変換が 2 つ表示されます。最初の変換には 1 つの接続（[nconns]）が関連付けられ、2 番めの変換には 4 つの接続が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	現在の変換および接続情報を消去します。
show conn	アクティブ接続をすべて表示します。
show local-host	ローカルホスト ネットワーク情報を表示します。
show uauth	現在認識されているユーザを表示します。