CHAPTER 30

show service-policy コマンド～ show xlate コマンド

show service-policy

サービス ポリシー統計情報を表示するには、特権 EXEC モードで **show service-policy** コマンドを使用します。

show service-policy [**global** | **interface** *intf*] [**csc** | **inspect** | **ips** | **police** | **priority** | **shape**]

show service-policy [**global** | **interface** *intf*] [**set connection** [**details**]]

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*]]

構文の説明

csc	（任意）**csc** コマンドを含むポリシーだけを出力します。
dest_ip dest_mask	トラフィック フローの宛先 IP アドレスおよびネットマスク。
details	（任意）クライアントごとの接続制限がイネーブルになっている場合は、クライアントごとの接続情報を表示します。
eq *dest_port*	（任意）等号。宛先ポートは、等号に続けて指定するポート番号と一致する必要があります。
eq *src_port*	（任意）等号。送信元ポートは、等号に続けて指定するポート番号と一致する必要があります。
flow *protocol*	（任意）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。*protocol* 引数の有効な値については、「使用上のガイドライン」を参照してください。
global	（任意）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	（任意）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* 引数の有効な値については、「使用上のガイドライン」を参照してください。
icmp_number	（任意）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	（任意）**inspect** コマンドを含むポリシーだけを出力します。
interface *intf*	（任意）*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	**ips** コマンドを含むポリシーだけを出力します。
police	**police** コマンドを含むポリシーだけを出力します。
priority	**priority** コマンドを含むポリシーだけを出力します。
set connection	**set connection** コマンドを含むポリシーだけを出力します。
shape	**shape** コマンドを含むポリシーだけを出力します。
src_ip src_mask	トラフィック フローで使用されている送信元 IP アドレスおよびネットマスク。

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 モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	**csc** キーワードが追加されました。
7.2(4)/8.0(4)	**shape** キーワードが追加されました。

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、サービス ポリシー コンフィギュレーションによって、必要なサービスが特定の接続に提供されることを確認できます。**flow** キーワードに続いて指定する引数とキーワードでは、オブジェクト グループ化されていないフローを IP 5 タプル形式で指定します。

IP 5 タプル形式でフローを指定するため、一部の一致基準はサポートされません。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送信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** コマンドによって定義されたトラフィック マッチングに一致するインターフェイスへの、初期接続の数を示しています。「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接続の制限値が表示されます。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** コマンドによって定義されたトラフィック タイプに一致すると、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* 引数の有効な値を示します。

- *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* 引数の有効な値を示します。

- **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

次に、**show service-policy global** コマンドの出力例を示します。

```
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
```

次に、**show service-policy priority** コマンドの出力例を示します。

```
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
```

次に、**show service-policy flow** コマンドの出力例を示します。

```
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
```

次に、**show service-policy inspect http** コマンドの出力例を示します。この例では、match-any クラスマップ内の match コマンドごとに統計情報が表示されます。

```
hostname# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

次に、**show service-policy inspect waas** コマンドの出力例を示します。この例では、waas の統計情報が表示されます。

```
hostname# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
       SYN with WAAS option 4
       SYN-ACK with WAAS option 4
       Confirmed WAAS connections 4
       Invalid ACKs seen on WAAS connections 0
       Data exceeding window size on WAAS connections 0
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
clear service-policy	すべてのサービス ポリシー コンフィギュレーションをクリアします。
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 ftp

FTP インスペクションの FTP 設定を表示するには、特権 EXEC モードで **show service-policy inspect ftp** コマンドを使用します。

show service-policy [**interface** *int*] **inspect ftp**

構文の説明

interface *int*	（任意）特定のインターフェイスを指定します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

FTP インスペクション中に、セキュリティ アプライアンスが何も通知せずにパケットをドロップする場合があります。セキュリティ アプライアンスの内部でパケットがドロップされているかどうかを確認するには、**show service-policy inspect ftp** コマンドを入力します。

（注）　値が 0 のドロップ カウンタはコマンド出力に表示されません。セキュリティ アプライアンスが何も通知せずにパケットをドロップすることはまれであるため、このコマンドの出力にドロップ カウンタが表示されることはほとんどありません。

表 30-1 に、**show service-policy inspect ftp** コマンドの出力を示します。

表 30-1　FTP ドロップ カウンタの説明

ドロップ カウンタ	カウンタ値の増分条件
Back port is zero drop	APPE、STOR、STOU、LIST、NLIST、RETR の各コマンドを処理するときにポート値が 0 である場合。
Can't allocate back conn drop	別のデータ接続を割り当てようとして失敗した場合。
Can't allocate CP conn drop	セキュリティ アプライアンスが CP 接続のデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないかどうかをチェックしてください。

表 30-1　FTP ドロップ カウンタの説明 （続き）

ドロップ カウンタ	カウンタ値の増分条件
Can't alloc FTP data structure drop	セキュリティ アプライアンスが FTP インスペクションのデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないか確認してください。
Can't allocate TCP proxy drop	セキュリティ アプライアンスが TCP プロキシのデータ構造を割り当てようとして失敗した場合。 システム メモリが不足していないか確認してください。
Can't append block drop	FTP パケットのスペース不足により、パケットにデータを追加できない場合。
Can't PAT port drop	セキュリティ アプライアンスがポートに PAT を設定するのに失敗した場合。
Cmd in reply mode drop	REPLY モードでコマンドを受信した場合。
Cmd match failure drop	セキュリティ アプライアンスで regex の照合時に内部エラーが発生した場合。 Cisco TAC にお問い合わせください。
Cmd not a cmd drop	FTP コマンド ストリングに数字などの無効な文字が含まれている場合。
Cmd not port drop	PORT コマンドを受信する予定のセキュリティ アプライアンスで別のコマンドを受信した場合。
Cmd not supported drop	セキュリティ アプライアンスでサポートされていない FTP コマンドを検出した場合。
Cmd not supported in IPv6 drop	IPv6 で FTP コマンドがサポートされていない場合。
Cmd not terminated drop	FTP コマンドが NL または CR で終了した場合。
Cmd retx unexpected drop	再送信されたパケットを予期せずに受信した場合。
Cmd too short drop	FTP コマンドが短すぎる場合。
ERPT too short drop	ERPT コマンドが短すぎる場合。
IDS internal error drop	FTP ID チェック中に内部エラーが発生した場合。 Cisco TAC にお問い合わせください。
Invalid address drop	インスペクション中に無効な IP アドレスが検出された場合。
Invalid EPSV format drop	ESPV コマンドで形式エラーが検出された場合。
Invalid ERPT AF number drop	ERPT コマンドの Address Family（AF; アドレス ファミリ）が無効な場合。
Invalid port drop	インスペクション中に無効なポートが検出された場合。
No back port for data drop	APPE、STOR、STOU、LIST、NLIST、RETR の各コマンドを処理しているときにパケットにポートが含まれていない場合。
PORT command/reply too long drop	PORT コマンドまたはパッシブ応答の長さが 8 を超えた場合。
Reply code invalid drop	応答コードが無効な場合。
Reply length negative drop	応答の長さの値が負である場合。
Reply unexpected drop	セキュリティ アプライアンスで、応答を予期していないときに応答を受信した場合。
Retx cmd in cmd mode drop	CMD モードで再送信されたコマンドを受信した場合。

表 30-1　FTP ドロップ カウンタの説明 （続き）

ドロップ カウンタ	カウンタ値の増分条件
Retx port not old port drop	パケットを再送信したが、パケット内のポートが最初に送信したポートとは異なる場合。
TCP option exceeds limit drop	TCP オプションの長さの値が原因で、オプションの長さが TCP ヘッダーの制限値を超える場合。
TCP option length error drop	TCP オプションの長さの値が正しくない場合。

例

次に、**show service-policy inspect ftp** コマンドの出力例を示します。

```
hostname# show show show service-policy inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ftp, packet 0, drop 0, reset-drop 0
               Can't alloc CP conn drop 1, Can't alloc proxy drop 2
               TCP option exceeds limit drop 3, TCP option length error drop 4
               Can't alloc FTP structure drop 1, Can't append block drop 2
               PORT cmd/reply too long drop 3, ERPT too short drop 4
               Invalid ERPT AF number drop 5, IDS internal error drop 6
               Invalid address drop 7, Invalid port drop 8
               Can't PAT port drop 9, Invalid EPSV format drop 10
               Retx port not old port drop 11, No back port for data drop 12
               Can't alloc back conn drop 13, Back port is zero drop 14
               Cmd too short drop 15, Cmd not terminated drop 16
               Cmd not a cmd drop 17, Cmd match failure drop 18
               Cmd not supported drop 19, Cmd not supported in IPv6 drop 20
               Cmd not port drop 21, Retx cmd in cmd mode drop 22
               Cmd retx unexpected drop 23, Cmd in reply mode drop 24
               Reply length negative drop 25, Reply unexpected drop 26
               Reply code invalid drop 27
```

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。
inspect ftp	FTP トラフィックを検査するアプリケーション インスペクションを設定します。

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*] }

構文の説明

apn	（任意）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	（任意）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 進数値。
interface	（任意）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	（任意）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 ネットワークと他のネットワーク間のインターフェイスです。
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）指定した 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	（任意）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	（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 統計情報を表示します。
tid	（任意）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 進数値。
version	（任意）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 モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　縦棒 | 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 の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、異なる GSN ノードにある 2 個の関連する PDP コンテキストによって定義され、1 つのトンネル ID によって識別されます。GTP トンネルは、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 ユーザの間でパケットを転送するために必要です。

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
```

次の例のように縦棒 | 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。

次に、GTP インスペクションの統計情報を表示するコマンドを示します。

```
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
```

次に、PDP コンテキストに関する情報を表示するコマンドを示します。

```
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 30-2 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各列の説明を示します。

表 30-2　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	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクション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	アプリケーション インスペクションに使用する特定の GTP マップを適用します。

show service-policy inspect radius-accounting

アプリケーション インスペクションの RADIUS アカウンティング設定を表示するには、特権 EXEC モードで **show service-policy inspect radius-accounting** コマンドを使用します。

show service-policy [**interface** *int*] **inspect radius-accounting**

構文の説明

interface *int*	（任意）特定のインターフェイスを指定します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show show service-policy inspect radius-accounting** コマンドの出力例を示します。

```
hostname# show show service-policy inspect radius-accounting
0 in use, 0 most used, 200 maximum allowed
```

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。
inspect radius-accounting	RADIUS アカウンティング トラフィックを検査するアプリケーション インスペクションを設定します。

show shun

shun 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*]

構文の説明

src_ip	（任意）このアドレスに関する情報を表示します。
statistics	（任意）インターフェイスのカウンタだけを表示します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show 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	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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。このコマンドは、**debug sip** および **show local-host** コマンドとともに、SIP インスペクション 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） **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** コマンドが最後まで出力されるまでに時間がかかります。

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、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 セッションが表示されています（`Total` フィールドを参照）。各 `call-id` が 1 つのコールを表します。

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、このセッションがまだコール設定中であることを示しています。コール設定が完了するのは、ACK が確認されてからです。このセッションは、1 秒間アイドル状態でした。

2 番めのセッションは Active 状態です。この状態ではコール設定が完了し、エンドポイントが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 インスペクション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）インスペクション 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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
```

この出力から、両方の内部 Cisco IP Phone の間でコールが確立されていることがわかります。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 接続に関する 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 インスペクション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 sla monitor configuration

デフォルトを含む、SLA 動作のコンフィギュレーション値を表示するには、ユーザ EXEC モードで **show sla monitor configuration** コマンドを使用します。

show sla monitor configuration [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作のコンフィギュレーション値が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションの SLA 動作コマンドを確認するには、**show running config sla monitor** コマンドを使用します。

例

次に、**show sla monitor** コマンドの出力例を示します。SLA 動作 123 のコンフィギュレーション値が表示されます。**show sla monitor** コマンドの出力に続いて、同じ SLA 動作の **show running-config sla monitor** コマンドが出力されます。

```
hostname> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
```

```
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

hostname# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show sla monitor operational-state

SLA 動作の動作状態を表示するには、ユーザ EXEC モードで **show sla monitor operational-state** コマンドを使用します。

show sla monitor operational-state [*sla-id*]

構文の説明

sla-id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合は、すべての SLA 動作の統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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
7.2(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

実行コンフィギュレーションの SLA 動作コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次に、**show sla monitor operational-state** コマンドの出力例を示します。

```
hostname> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。
sla monitor	SLA モニタリング動作を定義します。

show snmp-server statistics

SNMP サーバ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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

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	SNMP サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバ 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*]

構文の説明

ip_address	（任意）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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 だけをサポートしている場合、Version 列には 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 列には 1.99 が表示されます。SSH クライアントが SSH バージョン 2 だけをサポートしている場合、Version 列には 2.0 が表示されます。Encryption 列には、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 列には、クライアントとセキュリティ アプライアンスが行っている通信の進行状況が表示されます。[Username] には、この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。Mode 列には、SSH データ ストリームの方向が表示されます。SSH バージョン 2 の場合は、同じ暗号化アルゴリズムを使用することも、異なるアルゴリズムを使用することもできます。Mode フィールドには in および out が表示されます。SSH バージョン 1 の場合は、いずれの方向にも同じ暗号化を使用します。Mode フィールドには該当なしを表す記号（「-」）が表示され、1 つの接続に対して 1 つのエントリのみが表示されます。

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したり、スタートアップ コンフィギュレーションがロードされたときのエラーを表示したりするには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [errors]

構文の説明

errors	（任意）セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたエラーを表示します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

1. **errors** キーワードは、シングル モードおよびシステム実行スペースでだけ使用できます。

コマンド履歴

リリース	変更内容
7.0(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 モードでは、このコマンドを実行すると、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が表示されます。

スタートアップ エラーをメモリからクリアするには、**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.X(X)
!
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	スタートアップ エラーをメモリからクリアします。
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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 サービスで開かれ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の Sun リモート プロセッサ コール サービスをクリアします。
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クリアします。
inspect sunrpc	Sun RPC アプリケーション インスペクション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	SunRPC サービス コンフィギュレーションに関する情報を表示します。

show switch mac-address-table

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルでは、特権 EXEC モードで **show switch mac-address-table** コマンドを使用して、スイッチ MAC アドレス テーブルを表示します。

show switch mac-address-table

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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、組み込みスイッチを持つモデル専用です。スイッチ MAC アドレス テーブルには、スイッチ ハードウェア内の各 VLAN のトラフィックに適用する MAC アドレスとスイッチ ポートのマッピングが保持されます。トランスペアレント ファイアウォール モードでは、**show mac-address-table** コマンドを使用して ASA ソフトウェア内のブリッジ MAC アドレス テーブルを表示します。このブリッジ MAC アドレス テーブルには、VLAN 間を通過するトラフィックに適用する MAC アドレスと VLAN インターフェイスのマッピングが保持されます。

MAC アドレス エントリは 5 分経過するとエージング アウトします。

例

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

```
hostname# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic      | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic      | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic      | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic      | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static       |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast |  -  | In0/1,Et0/0-7
Total Entries: 6
```

表 30-3 に、各フィールドの説明を示します。

表 30-3　show switch mac-address-table のフィールド

フィールド	説明
Mac Address	MAC アドレスを表示します。
VLAN	MAC アドレスに関連付けられている VLAN を表示します。
Type	MAC アドレスを、ダイナミックに学習するか、スタティック マルチキャスト アドレスとして学習するか、またはスタティックに学習するかを示します。スタティック エントリは、内部バックプレーン インターフェイスの場合にのみ該当します。
Age	MAC アドレス テーブル内にあるダイナミック エントリの経過時間を表示します。
Port	この MAC アドレスのホストに到達できるスイッチ ポートを表示します。

関連コマンド

コマンド	説明
show mac-address-table	組み込みスイッチのないモデルの MAC アドレス テーブルを表示します。
show switch vlan	VLAN と物理 MAC アドレスの関連付けを表示します。

show switch vlan

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルでは、特権 EXEC モードで **show switch vlan** コマンドを使用して、VLAN および関連付けられているスイッチ ポートを表示します。

show switch vlan

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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、組み込みスイッチを持つモデル専用です。他のモデルの場合は、**show vlan** コマンドを使用します。

例

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

```
hostname# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                            up        Et0/0, Et0/1
200  outside                           up        Et0/7
300  -                                 down      Et0/1, Et0/2
400  backup                            down      Et0/3
```

表 30-4 に、各フィールドの説明を示します。

表 30-4　show switch vlan のフィールド

フィールド	説明
VLAN	VLAN 番号を表示します。
Name	VLAN インターフェイスの名前を表示します。**nameif** コマンドを使用して名前が設定されていない場合、または **interface vlan** コマンドが実行されていない場合は、ダッシュ（-）が表示されます。
Status	スイッチ内の VLAN とトラフィックを送受信するためのステータス（up または down）を表示します。VLAN がアップ状態になるには、その VLAN で少なくとも 1 つのスイッチ ポートがアップ状態である必要があります。
Ports	各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN にリストされている場合、そのポートはトランク ポートです。上記の出力例で、Ethernet 0/1 は VLAN 100 および VLAN 300 を伝送するトランク ポートです。

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。
interface vlan	VLAN インターフェイスを作成し、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実行時ステータスと統計情報を表示します。
show vlan	組み込みスイッチのないモデルの VLAN を表示します。
switchport mode	スイッチ ポートのモードをアクセス モードまたはトランク モードに設定します。

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 および IPv6 のアドレスをサポートします。

show tcpstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 28 に、表示される TCP 統計情報の説明を示します。

表 30-5　show tcpstat コマンドの TCP 統計情報

統計	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、ユーザ認可で使用されます。
tcp_xmt pkts	TCP スタックが送信したパケットの数。
tcp_rcv good pkts	TCP スタックが受信し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	チェックサムに誤りがあっ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 ユーザをハッシュ テーブルに追加しようとしたとき、そのユーザがすでにテーブル内に存在していた回数。
tcp user srch hash hit	検索時にハッシュ テーブル内で TCP ユーザが検出された回数。

表 30-5　show tcpstat コマンドの TCP 統計情報 （続き）

統計	説明
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザが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、そのユーザがハッシュ テーブル内で検出されなかった回数。
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。
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ビティ 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 ユーザの再送信回数。

例

次に、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**]

構文の説明

detail	（任意）詳細情報を表示します。
file	（任意）コマンドの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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**detail** キーワードおよび **file** キーワードが追加されました。
7.2(1)	出力表示が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。

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。テクニカル サポート アナリストは、このコマンドと各種 **show** コマンドの出力を組み合わせてさまざまな情報を入手します。

例

次に、実行コンフィギュレーションの出力を除外して、テクニカル サポートでの分析に使用する情報を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 cpu hogging process ------------------

Process:      fover_parse, NUMHOG: 2, MAXHOG: 280, LASTHOG: 140
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           11a4d5
Traceback:    12135e  121893  121822  a10d8b  9fd061  114de6 113e56f
              777135  7a3858  7a3f59  700b7f  701fbf  14b984

------------------ 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 サーバ（PFSS）および Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）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アクティブになっているセキュリティ アプライアンスを表示します。
show memory	物理メモリの最大量およびオペレーティング 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 threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにすると、特権 EXEC モードで **show threat-detection rate** コマンドを使用して統計情報を表示できます。

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

構文の説明

acl-drop	（任意）アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
bad-packet-drop	（任意）パケット形式に誤りがあって（invalid-ip-header または invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレートを表示します。
conn-limit-drop	（任意）接続制限（システム全体のリソース制限および設定された制限の両方）を超えたためにドロップされたパケットのレートを表示します。
dos-drop	（任意）DoS 攻撃（無効な SPI やステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレートを表示します。
fw-drop	（任意）基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	（任意）疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。
inspect-drop	（任意）アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。
interface-drop	（任意）インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。
scanning-threat	（任意）スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	（任意）TCP SYN 攻撃やデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 10 分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection rate** コマンドの出力例を示します。

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにした場合は、特権 EXEC モードで **show threat-detection scanning-threat** コマンドを使用すると、攻撃者および攻撃対象と分類されたホストが表示されます。

show threat-detection scanning-threat [**attacker** | **target**]

構文の説明

attacker	（任意）攻撃元ホストの IP アドレスを表示します。
target	（任意）攻撃対象ホストの IP 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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	見出しテキストに「& Subnet List」を表示するように変更されました。

例

次に、**show threat-detection scanning-threat** コマンドの出力例を示します。

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection shun	現在回避されているホストを表示します。

コマンド	説明
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection shun

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにし、攻撃元ホストを自動的に回避した場合は、特権 EXEC モードで **show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

show threat-detection shun

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドの出力例を示します。

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection statistics host

threat-detection statistics host コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics host** コマンドを使用するとホスト統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定のホストの統計情報を表示します。
mask	（任意）ホスト IP アドレスのサブネット マスクを設定します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

表 30-6 に、各フィールドの説明を示します。

表 30-6　show threat-detection statistics host のフィールド

フィールド	説明
Host	ホストの IP アドレスを表示します。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数を表示します。
act-ses	ホストが現在関係しているアクティブなセッションの合計数を表示します。

表 30-6　show threat-detection statistics host のフィールド （続き）

フィールド	説明
fw-drop	ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、およびデータなし UDP 攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。
null-ses	ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバからデータの送信がなかった UDP セッションです。
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌル セッション状態（上記を参照）であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在継続中の完了していないバースト間隔におけるイベントは、平均レートの計算に含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。

表 30-6　show threat-detection statistics host のフィールド （続き）

フィールド	説明
Total events	各レート間隔におけるイベントの合計数を表示します。現在途中である未完了のバースト間隔は、合計イベント数には含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ホストから正常に送信されたバイト数を表示します。
Sent pkts	ホストから正常に送信されたパケット数を表示します。
Sent drop	ホストから送信されたパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。
Recv byte	ホストが正常に受信したバイト数を表示します。
Recv pkts	ホストが正常に受信したパケット数を表示します。
Recv drop	ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics port

threat-detection statistics port コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics port** コマンドを使用すると、TCP ポートおよび UDP ポートの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]

構文の説明

start_port[**-***end_port*]	（任意）0 ～ 65535 の間の特定のポートまたはポート範囲の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics port** コマンドの出力例を示します。

```
hostname# show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

表 30-7 に、各フィールドの説明を示します。

表 30-7　show threat-detection statistics port のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。

表 30-7　show threat-detection statistics port のフィールド （続き）

フィールド	説明
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
tot-ses	このポートのセッションの合計数を表示します。
act-ses	ポートが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ポートから正常に送信されたバイト数を表示します。
Sent pkts	ポートから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、ポートから送信されたパケット数を表示します。
Recv byte	ポートが正常に受信したバイト数を表示します。
Recv pkts	ポートが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、ポートが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics protocol

threat-detection statistics protocol コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics protocol** コマンドを使用すると、IP プロトコルの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

構文の説明

protocol_number	（任意）0 ～ 255 の間の特定のプロトコル番号の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
protocol_name	（任意）特定のプロトコル名の統計情報を表示します。 • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics protocol** コマンドの出力例を示します。

```
hostname# show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

表 30-8 に、各フィールドの説明を示します。

表 30-8　show threat-detection statistics protocol のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
protocol_number/ *protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。
tot-ses	このプロトコルのセッションの合計数を表示します。
act-ses	プロトコルが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、 8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	プロトコルから正常に送信されたバイト数を表示します。
Sent pkts	プロトコルから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、プロトコルから送信されたパケット数を表示します。
Recv byte	プロトコルが正常に受信したバイト数を表示します。

表 30-8　show threat-detection statistics protocol のフィールド （続き）

フィールド	説明
Recv pkts	プロトコルが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、プロトコルが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics top

threat-detection statistics コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics top** コマンドを使用すると、上位 10 件の統計情報が表示されます。特定のタイプで脅威の検出の統計情報がイネーブルでない場合、このコマンドではそれらの統計情報を表示できません。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**]]

構文の説明

access-list	（任意）許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
all	（任意）TCP 代行受信の場合、追跡されたすべてのサーバの履歴データを表示します。
detail	（任意）TCP 代行受信の場合、サンプリング データの履歴を表示します。
host	（任意）一定期間ごとに上位 10 件のホスト統計情報を表示します。 **（注）** 脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
port-protocol	（任意）TCP/UDP ポート タイプと IP プロトコル タイプを組み合わせた上位 10 件の統計情報を表示します。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
rate-1	（任意）表示されている一定レート間隔のうち、最小のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-1** キーワードを使用すると、1 時間間隔だけがセキュリティ アプライアンスに表示されます。
rate-2	（任意）表示されている一定レート間隔のうち、中間のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-2** キーワードを使用すると、8 時間間隔だけがセキュリティ アプライアンスに表示されます。

rate-3	（任意）表示されている一定レート間隔のうち、最大のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-3** キーワードを使用すると、24 時間間隔だけがセキュリティ アプライアンスに表示されます。
tcp-intercept	TCP 代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバが含まれます。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 最後に完了したバースト間隔における現行のバースト レート（イベント/秒）。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

セキュリティ アプライアンスは、平均レート間隔内でイベント カウントを 60 回計算します。つまりセキュリティ アプライアンスは、合計 60 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

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

```
hostname# show threat-detection statistics top access-list

                    Top     Average(eps)     Current(eps) Trigger         Total events
```

```
1-hour ACL hits:
            100/3[0]             173              0        0              623488
            200/2[1]              43              0        0              156786
            100/1[2]              43              0        0              156786
8-hour ACL hits:
            100/3[0]              21           1298        0              623488
            200/2[1]               5            326        0              156786
            100/1[2]               5            326        0              156786
```

表 30-9 に、各フィールドの説明を示します。

表 30-9　show threat-detection statistics top access-list のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、時間内の ACE のランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示される ACE が 10 件未満となります。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 60 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	最後に完了したバースト間隔における現行のバースト レート（イベント/秒）を表示します。バースト間隔は、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の間隔です。Average(eps) の説明の例では、現在のレートは 3:19:30 から 3:20:00 となります。
Trigger	アクセス リスト トラフィックがトリガーするレート制限は設定されていないため、この列は常に 0 です。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。この規則での唯一の例外は、合計イベントを計算する時点で、完了していないバースト間隔内でのイベント数が最も古いバースト間隔（60 間隔中の 1 番目）をすでに超過している場合です。この場合、セキュリティ アプライアンスは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
1-hour、8-hour	これらの固定レート間隔における統計情報を表示します。
acl_name/line_number	拒否される原因となった ACE のアクセス リスト名および行番号を表示します。

次に、**show threat-detection statistics top access-list rate-1** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top access-list rate-1

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
               100/3[0]              173                0       0                623488
               200/2[1]               43                0       0                156786
               100/1[2]               43                0       0                156786
```

次に、**show threat-detection statistics top port-protocol** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top port-protocol

Top           Name    Id    Average(eps)     Current(eps) Trigger      Total events
  1-hour Recv byte:
 1          gopher    70              71                0       0          32345678
 2   btp-clnt/dhcp    68              68                0       0          27345678
 3          gopher    69              65                0       0          24345678
 4     Protocol-96 * 96              63                0       0          22345678
 5       Port-7314 7314              62                0       0          12845678
 6 BitTorrent/trc 6969              61                0       0          12645678
 7      Port-8191-65535             55                0       0          12345678
 8            SMTP  366             34                0       0           3345678
 9          IPinIP *  4             30                0       0           2345678
10           EIGRP * 88             23                0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

表 30-10 に、各フィールドの説明を示します。

表 30-10　show threat-detection statistics top port-protocol のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるポートまたはプロトコルのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるポート/プロトコルが 10 件未満となります。
Name	ポートまたはプロトコル名を表示します。
Id	ポート ID 番号またはプロトコル ID 番号を表示します。アスタリスク（*）は、その ID が IP プロトコル番号であることを意味します。
Average(eps)	表 30-6 の説明を参照してください。
Current(eps)	表 30-6 の説明を参照してください。

表 30-10　show threat-detection statistics top port-protocol のフィールド （続き）

フィールド	説明
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	表 30-6 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたポートおよびプロトコルから正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたポートおよびプロトコルから正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたポートおよびプロトコルから送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたポートおよびプロトコルで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
protocol_number/*protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。

次に、**show threat-detection statistics top host** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top host

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
         10.0.0.1[0]             2938                0       0              10580308
  1-hour Sent pkts:
         10.0.0.1[0]               28                0       0                104043
  20-min Sent drop:
         10.0.0.1[0]                9                0       1                 10851
  1-hour Recv byte:
         10.0.0.1[0]             2697                0       0               9712670
  1-hour Recv pkts:
         10.0.0.1[0]               29                0       0                104846
  20-min Recv drop:
         10.0.0.1[0]               42                0       3                 50567
  8-hour Sent byte:
         10.0.0.1[0]              367                0       0              10580308
  8-hour Sent pkts:
         10.0.0.1[0]                3                0       0                104043
  1-hour Sent drop:
         10.0.0.1[0]                3                0       1                 10851
  8-hour Recv byte:
         10.0.0.1[0]              337                0       0               9712670
  8-hour Recv pkts:
         10.0.0.1[0]                3                0       0                104846
  1-hour Recv drop:
         10.0.0.1[0]               14                0       1                 50567
```

```
24-hour Sent byte:
         10.0.0.1[0]             122              0       0             10580308
24-hour Sent pkts:
         10.0.0.1[0]               1              0       0               104043
24-hour Recv byte:
         10.0.0.1[0]             112              0       0              9712670
24-hour Recv pkts:
         10.0.0.1[0]               1              0       0               104846
```

表 30-11 に、各フィールドの説明を示します。

表 30-11　show threat-detection statistics top host のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるホストのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるホストが 10 件未満となります。
Average(eps)	表 30-6 の説明を参照してください。
Current(eps)	表 30-6 の説明を参照してください。
Trigger	表 30-6 の説明を参照してください。
Total events	表 30-6 の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたホストに正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたホストに正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたホストに送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたホストで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
host_ip_address	パケットまたはバイトが送信、受信、ドロップされたホスト IP アドレスを表示します。

次に、**show threat-detection statistics top tcp-intercept** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
```

```
10    192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

表 30-12 に、各フィールドの説明を示します。

表 30-12　show threat-detection statistics top tcp-intercept のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにセキュリティ アプライアンスがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。この間隔の間に、セキュリティ アプライアンスはデータを 60 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常に 60 で割ったレート間隔です。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	サンプリング期間中の平均攻撃レートを 1 秒あたりの攻撃数で表示します。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip	攻撃者の IP アドレスを表示します。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。

次に、**show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。

```
hostname# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
----------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (60 Samplings):
              95348      95337      95341      95339      95338      95342
              95337      95348      95342      95338      95339      95340
              95339      95337      95342      95348      95338      95342
              95337      95339      95340      95339      95347      95343
              95337      95338      95342      95338      95337      95342
              95348      95338      95342      95338      95337      95343
              95337      95349      95341      95338      95337      95342
              95338      95339      95338      95350      95339      95570
              96351      96351      96119      95337      95349      95341
              95338      95337      95342      95338      95338      95342
......
```

表 30-13 に、各フィールドの説明を示します。

表 30-13　show threat-detection statistics top tcp-intercept detail のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにセキュリティ アプライアンスがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval** コマンドを使用します。この間隔の間に、セキュリティ アプライアンスはデータを 60 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常に 60 で割ったレート間隔です。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	**threat-detection statistics tcp-intercept rate-interval** コマンドで設定されたレート間隔での平均攻撃レートを、1 秒あたりの攻撃数で表示します（デフォルトのレート間隔は 30 分です）。レート間隔中、セキュリティ アプライアンスは 30 秒ごとにデータをサンプリングします。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip or <*various*> Last: *attacker_ip*	攻撃者の IP アドレスを表示します。複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。
sampling data	60 個のサンプリング データ値をすべて表示します。これらの値は、間隔ごとの攻撃数を示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show tls-proxy

TLS プロキシおよびセッ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 モードで **show tls-proxy** コマンドを使用します。

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**]]

構文の説明

cert-dump	ローカル ダイナミック証明書をダンプします。出力は LDC の 16 進ダンプです。
count	セッション カウンタだけを表示します。
detail	各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。
host *host_addr*	関連付けられたセッションを表示する特定のホストを指定します。
session	アクティブな TLS プロキシ セッションを表示します。
tls_name	表示する TLS プロキシの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、**show tls-proxy** コマンドの出力例を示します。

```
hostname# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

次に、**show tls-proxy session** コマンドの出力例を示します。

```
hostname# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

次に、**show tls-proxy session detail** コマンドの出力例を示します。

```
hostname# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show running-config tls-proxy	すべてまたは指定された TLS プロキシの実行コンフィギュレーションを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

show track

トラッキング プロセスが追跡したオブジェクトに関する情報を表示するには、ユーザ EXEC モードで **show track** コマンドを使用します。

show track [*track-id*]

構文の説明

track-id	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

track-id が指定されなかった場合は、すべてのトラッキング オブジェクトに関する情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show track** コマンドの出力例を示します。

```
hostname(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

関連コマンド

コマンド	説明
show running-config track	実行コンフィギュレーションの **track rtr** コマンドを表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5550 適応型セキュリティ アプライアンスのための特別な表示が追加されました。

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前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

ASA 5550 適応型セキュリティ アプライアンスの場合、**show traffic** コマンドを実行するとスロットごとの集約スループットも表示されます。ASA 5550 適応型セキュリティ アプライアンスのスループットを最大にするには、トラフィックをスロットに均一に分散する必要があります。この表示は、トラフィックが均一に分散しているかどうかを確認するのに役立ちます。

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
```

ASA 5550 適応型セキュリティ アプライアンスの場合、次のテキストが最後に表示されます。

```
----------------------------------------
        Per Slot Throughput Profile
----------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************

  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

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

現在認証済みの 1 名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 とポートの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*]

構文の説明

username	（任意）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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show uauth コマンドは、1 名またはすべてのユーザの AAA 認可キャッシュおよび認証キャッシュを表示します。

このコマンドは、**timeout** コマンドとともに使用します。

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。このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、セキュリティ アプライアンスではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。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、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）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

show uauth コマンドの出力には、認証と認可のために認可サーバに渡されたユーザ名、そのユーザ名がバインドされている IP アドレス、およびこのユーザが認証されたのみであるか、または、キャッシュされたサービスがあ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、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 エントリが作成できません。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、いずれのユーザも認証されておらず、かつ、1 つのユーザ認証が進行している場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
                        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ており、かつ、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が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	アイドル時間の最大継続期間を設定します。

show url-block

url-block バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）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**]

構文の説明

block statistics	（任意）ブロック バッファの使用状況に関する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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 バッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）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
```

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 バッファの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 サーバに送ります。
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 または Websense のフィルタリング サーバから受信した URL 応答に使用される 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show url-cache statistics コマンドには、次のエントリが表示されます。

- Size：キャッシュ サイズ（KB 単位）。**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：キャッシュに含まれる現在のエントリ数。
- 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 コマンドを使用すると、N2H2 Sentian または Websense のフィルタリング 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 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 サーバに送ります。
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 サーバから受信した応答の 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバのベンダーおよびステータスを表示します。また、URL、HTTPS 接続、および TCP 接続について、合計数、許可された数、拒否された数を表示します。

show url-server コマンドには、次の情報が表示されます。

- 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
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
```

```
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                       DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                  Sent    Received
STATUS_REQUEST           411     0
LOOKUP_REQUEST           366519  365952
LOG_REQUEST              0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis.  The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

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 サーバに送ります。
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、ハードウェア構成、ライセンス キー、および関連する動作期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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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です。
7.2(1)	ステートフル フェールオーバー モードでは、クラスタの動作期間を示す追加の行が表示されます。

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。

- 以前のリリースにダウングレードした場合、現在のリリースのキーでは、以前のリリースでサポートされている数よりも多くのセキュリティ コンテキストが使用できる場合があります。キーのセキュリティ コンテキストの値がプラットフォームの制限を超えると、show activation-key の出力に次のメッセージが表示されます。

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

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

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

フェールオーバー クラスタの動作期間の値は、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 台のユニットが動作を停止しても、アクティブなユニットが動作を継続する限り、動作期間の値は増加し続けます。このため、フェールオーバー クラスタの動作期間を個別のユニットの動作期間よりも長くすることができます。フェールオーバーを一時的にディセーブルにしてから再びイネーブルにすると、フェールオーバーがディセーブルになる前のユニットの稼働時間と、フェールオーバーがディセーブルである間のユニットの稼働時間が加算されて、フェールオーバー クラスタの動作期間がレポートされます。

例

次に、ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連する動作期間の情報を表示する例を示します。ステートフル フェールオーバーが設定されている環境では、フェールオーバー クラスタの動作期間を示す追加の行が表示されます。フェールオーバーが設定されていない場合、この行は表示されません。

```
hostname# show version

Cisco Adaptive Security Appliance Software Version 8.0(0)
Device Manager Version 6.0(0)

Compiled on Mon 16-April-07 03:29 by root
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/main_backup.cfg"

hostname up 2 days 10 hours
failover cluster up 2 days 11 hours

Hardware:   ASA5520, 1024 MB RAM, CPU Pentium 4 Celeron 2000 MHz
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.01
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.04
 0: Ext: GigabitEthernet0/0  : address is 000b.fcf8.c44e, irq 9
 1: Ext: GigabitEthernet0/1  : address is 000b.fcf8.c44f, irq 9
 2: Ext: GigabitEthernet0/2  : address is 000b.fcf8.c450, irq 9
 3: Ext: GigabitEthernet0/3  : address is 000b.fcf8.c451, irq 9
 4: Ext: Management0/0       : address is 000b.fcf8.c44d, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 150
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 10
GTP/GPRS                     : Enabled
VPN Peers                    : 750
WebVPN Peers                 : 500
Advanced Endpoint Assessment : Disabled

This platform has an ASA 5520 VPN Plus license.

Serial Number: P3000000098
Running Activation Key: 0x7c2e394b 0x0c842e53 0x98f3edf0 0x8c1888b0 0x0336f1ac
Configuration register is 0x1
```

```
Configuration last modified by enable_15 at 14:17:59.410 EST Wed April 16 2007
hostname#
```

eject コマンドを実行した後、デバイスが物理的に取り外されていない状態で **show version** コマンドを入力すると、次のメッセージが表示されます。

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

関連コマンド

コマンド	説明
eject	外部コンパクト フラッシュ デバイスを、セキュリティ アプライアンスから物理的に取り外す前にシャットダウンできるようにします。
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 アプライアンスの稼働時間を表示します。

show vlan

セキュリティ アプライアンスに設定されているすべての VLAN を表示するには、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

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、設定されている VLAN を表示する例を示します。

```
hostname# 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。
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実行時ステータスと統計情報を表示します。

show vpn load-balancing

VPN ロード バランシングの仮想クラスタ 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

構文の説明

このコマンドには、変数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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
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。
7.1(1)	出力例の Load (%) 表示および Session 表示に、個別の IPSec 列および SSL 列が追加されました。

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、このコマンドはデバイスに 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。

ロードバランシング クラスタのマスターは、アクティブな AnyConnect セッション、クライアントレス セッション、そして設定された制限またはライセンス数制限に基づく最大許可セッションがあるクラスタ内の各 ASA からメッセージを定期的に受信します。クラスタ内のある ASA の容量が 100% いっぱいであると示される場合、クラスタ マスターはこれに対してさらに接続をリダイレクトすることはできません。ASA がいっぱいであると示されても、ユーザによっては非アクティブまたは再開待ち状態となり、ライセンスを消費する可能性があります。回避策として、セッション合計数ではなく、セッション合計数から非アクティブ状態のセッション数を引いた数が各 ASA によって提供されます つまり、非アクティブなセッションはクラスタ マスターに報告されません。ASA が（非アクティブなセッションによって）いっぱいになっている場合でも、クラスタ マスターは必要に応じて接続を ASA に引き続きリダイレクトします。ASA が新しい接続を受信すると、最も長く非アクティブになっていたセッションがログオフされ、新しい接続がそのライセンスを引き継ぎます。

出力にあるアスタリスク（*）は、接続先のセキュリティ アプライアンスの IP アドレスを示します。

例

次に、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場合の **show vpn load-balancing** コマンドの出力例を示します。

```
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
                                              Load (%)           Sessions
Public IP       Role   Pri     Model          IPSec  SSL        IPSec   SSL
------------------------------------------------------------------------------
* 192.168.1.40  Master 10      PIX-515         0       0          0       0
  192.168.1.110  Backup   5 PIX-515           0       0          0       0
hostname(config-load-balancing)#
```

（注） 非アクティブなセッションは最長時間から最短時間の順にソートされます。非アクティブな SSL セッションはカウントされないため、セッションとロードの合計には表示されません。

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** コマンドには次のような異なる結果が表示されます。

```
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 ステートメントを削除します。
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 モードを開始します。

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 **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他、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。使用可能なオプションについては、「構文の説明」および「使用上のガイドライン」を参照してください。

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* | **webvpn | email-proxy | svc} [filter {name** *username* | **ipaddress** *IPaddr* | **a-ipaddress** *IPaddr* | **p-ipaddress** *IPaddr* | **tunnel-group** *groupname* | **protocol** *protocol-name* | **encryption** *encryption-algo* | **inactive}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption | inactivity}]**

構文の説明

表示の詳細度	説明
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詳細情報が表示されます。 **detail** および **full** オプションを指定すると、セキュリティ アプライアンスではマシンで読み取り可能な形式で詳細な出力を表示します。
filter *filter_criteria*	（任意）1 つまたは複数のフィルタ オプションを使用して、指定する情報だけ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、「使用上のガイドライン」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。出力のレコード間には | 文字と || ストリングが表示されます。
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	**説明**
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。
svc	SSL VPN クライアント属性を設定します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(0)	VLAN フィールドの説明が追加されました。
7.2(1)	このコマンドが導入されました。
8.0(5)	**filter** オプションとして **inactive** および **sort** オプションとして **inactivity** 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	説明
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）に関する情報だけを表示します。
sort a-ipaddress	割り当て済み IP アドレスで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関する情報だけを表示します。
sort encryption	暗号化アルゴリズムで表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
filter inactive	接続が切断された非アクティブなセッションをフィルタリングします。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションがアクティブな場合、00:00m:00s が表示されます。
sort inactivity	非アクティブなセッションをソートします。
filter ipaddress *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）に関する情報だけを表示します。
sort ipaddress	内部 IP アドレスで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）のセッションを表示します。
sort name	ユーザ名のアルファベット順に表示内容をソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスに関する情報だけを表示します。
sort p-address	指定した外部 IP アドレス（複数可）で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関する情報だけを表示します。

フィルタ / ソート オプション	説明
sort protocol	プロトコルで表示内容をソートします。プロトコルには、IKE、IMAP4S、IPSec、IPSecLAN2LAN、IPSecLAN2LANOverNatT、IPSecOverNatT、IPSecoverTCP、IPSecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN が含まれます。
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）に関する情報だけを表示します。
sort tunnel-group	トンネル グループで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#
```

次の例は単一セッションの詳細を示します。

```
AsaNacDev# show vpn-sessiondb detail full index 4
Session Type: Remote Detailed |

Index: 2 | EasyVPN: 0 | Username: uuuu | Group: DfltGrpPolicy | Tunnel Group:
regr3000multigroup | IP Addr: 192.168.2.80 | Public IP: 161.44.173.216 | Protocol:
IPSecOverUDP | Encryption: 3DES | Login Time: 12:51:54 EDT Wed Jun 21 2006 |Duration:
0h:02m:44s | Bytes Tx: 2134 | Bytes Rx: 8535 | Client Type: WinNT | Client Ver: 4.0.5
(Rel) | Filter Name:  | NAC Result: N/A | Posture Token: : | VM Result: Static | VLAN: 10
||

IKE Sessions: 1
 | IPSecOverUDP Sessions: 1
 |

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeys | UDP Source Port: 500 |
UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES | Hashing:
SHA1 | Diffie-Hellman Group: 2 | Rekey Time Interval: 40000 Seconds| Rekey Left(T): 39836
Seconds ||

Type: IPSecOverUDP | Session ID: 2 | Local IP Addr: 0.0.0.0/0.0.0.0/0/0 | Remote IP Addr:
192.168.2.80/255.255.255.255/0/0 | Encryption: 3DES | Hashing: SHA1 | Encapsulation:
Tunnel | UDP Destination Port: 10000 | Rekey Time Interval: 28800 Seconds | Rekey Left(T):
28636 Seconds | Idle Time Out: 30 Minutes | Idle TO Left: 30 Minutes | Bytes Tx: 2134 |
Bytes Rx: 8535 | Packets Tx: 15 | Packets Rx: 2134 | ||

VLAN Mapping: VLAN: 10 |

AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : dbrownhi
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPSec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPSec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
```

```
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds           Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                       Bytes Rx     : 604533
  Pkts Tx      : 0                       Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds            Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds             EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds               Posture Token: Healthy
  Redirect URL : www.cisco.com
```

例に示すとおり、**show vpn-sessiondb** コマンドの応答に表示されるフィールドは、入力するキーワードによって異なります。表 30-14 に、これらのフィールドの説明を示します。

表 30-14　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Auth Mode	このセッションを認証するためのプロトコルまたはモード。
Bytes Rx	セキュリティ アプライアンスがリモートのピアまたはクライアントから受信した合計バイト数。
Bytes Tx	セキュリティ アプライアンスがリモートのピアまたはクライアントに送信した合計バイト数。
Client Type	リモート ピア上で実行されるクライアント ソフトウェア（利用できる場合）。
Client Ver	リモート ピア上で実行されるクライアント ソフトウェアのバージョン。
Connection	接続名またはプライベート IP アドレス。
D/H Group	Diffie-Hellman グループ。IPSec SA 暗号キーを生成するためのアルゴリズムおよびキー サイズ。
Duration	セッションのログイン時刻から直前の画面リフレッシュまでの経過時間（HH:MM:SS）。
EAPoUDP Session Age	正常に完了した直前のポスチャ確認からの経過秒数。
Encapsulation	IPSec Encapsulation Security Payload（ESP; 暗号ペイロード）プロトコルの暗号化と認証（つまり、ESP を適用した元の IP パケットの一部）を適用するためのモード。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム（ある場合）。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム。
EoU Age (T)	EAPoUDP セッションの経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
Filter Name	セッション情報の表示を制限するよう指定されたユーザ名。
Hashing	パケットのハッシュを生成するためのアルゴリズム。IPSec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
Hold-Off Time Remaining	直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
IKE Neg Mode	キー情報を交換し、SA を設定するための IKE（IPSec フェーズ 1）モード（アグレッシブまたはメイン）。

表 30-14　show vpn-sessiondb コマンドのフィールド （続き）

フィールド	説明
IKE Sessions	IKE（IPSec フェーズ 1）セッションの数で、通常は 1。これらのセッションにより、IPSec トラフィックのトンネルが確立されます。
Index	このレコードの固有識別情報。
IP Addr	このセッションのリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。
IPSec Sessions	IPSec（フェーズ 2）セッション（トンネル経由のデータ トラフィック セッション）の数。各 IPSec リモート アクセス セッションには、2 つの IPSec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
Local IP Addr	トンネルのローカル エンドポイント（セキュリティ アプライアンス上のインターフェイス）に割り当てられた IP アドレス。
Login Time	セッションがログインした日付と時刻（MMM DD HH:MM:SS）。時刻の表示は 24 時間表示です。
NAC Result	ネットワーク アドミッション コントロール ポスチャ検証の状態。次のいずれかを指定できます。 • [Accepted] : ACS は正常にリモート ホストのポスチャを検証しました。 • [Rejected] : ACS はリモート ホストのポスチャの検証に失敗しました。 • [Exempted] : セキュリティ アプライアンスに設定されたポスチャ検証免除リストに従って、リモート ホストはポスチャ検証を免除されました。 • [Non-Responsive] : リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。 • [Hold-off] : ポスチャ検証に成功した後、セキュリティ アプライアンスとリモート ホストの EAPoUDP 通信が途絶えました。 • [N/A] : VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。 • [Unknown] : ポスチャ検証が進行中です。
NAC Sessions	ネットワーク アドミッション コントロール（EAPoUDP）セッションの数。
Packets Rx	セキュリティ アプライアンスがリモート ピアから受信したパケット数。
Packets Tx	セキュリティ アプライアンスがリモート ピアに送信したパケット数。
PFS Group	完全転送秘密グループ番号。
Posture Token	Access Control Server 上で設定可能な情報テキスト ストリング。ACS は情報提供のためにセキュリティ アプライアンスにポスチャ トークンをダウンロードし、システム モニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。

表 30-14　show vpn-sessiondb コマンドのフィールド（続き）

フィールド	説明
Redirect URL	ポスチャ検証またはクライアントレス認証に続いて、ACS はセッションのアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。セキュリティ アプライアンスは、リモート ホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、セキュリティ アプライアンスはリモート ホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。 Redirect URL は、IPSec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。
Rekey Int (T)	IPSec（IKE）SA 暗号キーの有効期限。
Rekey Left (T)	IPSec（IKE）SA 暗号キーの残りのライフタイム。
Rekey Time Interval	IPSec（IKE）SA 暗号キーの有効期限。
Remote IP Addr	トンネルのリモート エンドポイント（リモート ピア上のインターフェイス）に割り当てられた IP アドレス。
Reval Int (T)	Revalidation Time Interval。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Reval Left (T)	Time Until Next Revalidation。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Session ID	セッション コンポーネント（サブセッション）の ID。各 SA には独自の ID があります。
Session Type	セッションのタイプ（LAN-to-LAN または Remote）。
SQ Int (T)	Status Query Time Interval。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Tunnel Group	属性値を求めるために、このトンネルが参照するトンネル グループの名前。
UDP Dst Port または UDP Destination Port	リモート ピアが使用する UDP のポート番号。

表 30-14　show vpn-sessiondb コマンドのフィールド （続き）

フィールド	説明
UDP Src Port または UDP Source Port	セキュリティ アプライアンスが使用する UDP のポート番号。
Username	セッションを確立したユーザのログイン名。
VLAN	このセッションに割り当てられた出力 VLAN インターフェイス。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この VLAN に転送します。次のいずれかの要素で値を指定します。 • グループ ポリシー • 継承されたグループ ポリシー

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、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、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***]**

構文の説明

encryption	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化に関して指定します。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の比率を表示します。
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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、引数として **encryption** を指定した場合の **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、引数として **protocol** を指定した場合の **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%
L2TP                     0               0%
L2TPOverIPSec            0               0%
L2TPOverIPSecOverNatT    0               0%
PPPoE                    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

IPSec、Cisco AnyConnect、および NAC の各セッションの数を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(0)	VLAN マッピング セッション テーブルが追加されました。
7.2(1)	このコマンドが導入されました。
8.0(5)	アクティブ、累積、ピーク同時、および非アクティブのセッションに関する出力が新たに追加されました。

例

次に、アクティブなデバイス上での **show vpn-sessiondb summary** コマンドの出力例を示します。

（注） スタンバイ状態のデバイスでは、アクティブなセッションと非アクティブなセッションが区別されません。

```
hostname# show vpn-sessiondb summary

Active Session Summary
Sessions:
                  Active :Cumulative :Peak Concurrent :Inactive :
  SSL VPN   :          0 :         1 :               1 :
    Clientless only    0 :         0 :               0 :        0
    With client        6 :         6 :               1 :        4
Totals                 0 :        10

License Information:
    Shared VPN License Information:
        SSL VPN                      : 12000
            Allocated to this device  :    0
            Allocated to network      :    0
            Device limit              : 750

IPsec   :   750     Configured :750    Active : 0     Load : 0%
SSL VPN :   750     Configured :750    Active : 0     Load : 0%
                        Active : Cumulative : Peak Concurrent
```

```
SSL VPN         :           6 :         1 :             1
Totals          :           0 :        10 :

Active NAC Sessions:
  Accepted                : 0
  Rejected                : 0
  Exempted                : 0
  Non-responsive          : 0
Hold-off                : 0
  N/A                     : 0

Active VLAN Mapping Sessions:
  Static                  : 0
  Auth                    : 0
  Access                  : 0
  Guest                   : 0
  Quarantine              : 0
  N/A                     : 0

F1-asa1#
```

セッションとは、特定のピアとの間で確立された VPN トンネルです。IPSec LAN-to-LAN トンネルは 1 セッションとしてカウントされ、このトンネル経由で複数のホスト間接続が可能になります。IPSec リモート アクセス セッションは、1 つのユーザ接続をサポートする 1 リモート アクセス トンネルです。

Active SSL VPN With Client カラムには、データを渡すことのできるアクティブな SSL トンネル セッションの数が表示されます。非アクティブ カラムには SSL トンネル セッションを失っているため、データを渡すことができないセッションが表示されます。非アクティブなセッションは後の時点で接続を再開する場合があります。ロード バランシングのため、非アクティブなセッションはマスターへの負荷として報告されません。たとえば、1 つのクラスタ メンバーに合計 10 件のセッションがあり、うち 6 つがアクティブ、4 つが非アクティブの場合、マスターに報告される負荷は 6 セッションです。

Total SSL VPN カラムには、アクティブなセッションと非アクティブなセッションの両方が表示されます。

（注） アクティブなセッションも非アクティブなセッションも、これまでと同様にライセンスを必要とします。デバイスの既存のセッションは、状態に関係なくライセンスを必要とします。

SSL VPN With Client の Cumulative 列には、確立されているアクティブなセッションの数が表示されます。SSL VPN With Client の Peak Concurrent 列には、データを送信中で、同時にアクティブなセッションのピーク数が表示されます。

表 30-15 に、Active Sessions テーブルと Session Information テーブルにあるフィールドの説明を示します。

表 30-15　show vpn-sessiondb summary コマンド：Active Sessions および Session Information のフィールド

フィールド	説明
Concurrent Limit	このセキュリティ アプライアンス上で許可された、同時にアクティブなセッションの最大数。
Cumulative Sessions	セキュリティ アプライアンスが最後に起動またはリセットされたとき以降のすべてのタイプのセッション数。
LAN-to-LAN	現在アクティブな IPSec LAN-to-LAN セッションの数。

表 30-15　show vpn-sessiondb summary コマンド：Active Sessions および Session Information のフィールド（続き）

フィールド	説明
Peak Concurrent	セキュリティ アプライアンスが最後に起動またはリセットされたとき以降に同時にアクティブであった、すべてのタイプのセッションの最大数。
Percent Session Load	使用中の vpn セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。利用可能なセッションの最大数は、次のいずれかの値です。 • ライセンスのある IPSec セッションおよび SSL VPN セッションの最大数 • 次のコマンドを使用して設定されたセッションの最大数 – **vpn-sessiondb max-session-limit** – **vpn-sessiondb max-webvpn-session-limit**
Remote Access	現在アクティブな PPTP、L2TP、IPSec リモート アクセス ユーザ、L2TP over IPSec、および IPSec through NAT の各セッションの数。
Total Active Sessions	現在アクティブなすべてのタイプのセッションの数。

Active NAC Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative NAC Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 30-16 に、Active NAC Sessions テーブルおよび Total Cumulative NAC Sessions テーブルにあるフィールドの説明を示します。

表 30-16　show vpn-sessiondb summary コマンド：Active NAC Sessions および Total Cumulative NAC Sessions のフィールド

フィールド	説明
Accepted	ポスチャ検証が成功し、Access Control Server によってアクセス ポリシーが付与されたピアの数。
Exempted	セキュリティ アプライアンス上に設定されたポスチャ検証免除リストのエントリに一致しているため、ポスチャ検証の対象とならないピアの数。
Hold-off	セキュリティ アプライアンスがポスチャ検証に成功した後、EAPoUDP 通信が途絶えたピアの数。このタイプのイベントが発生してから各ピアに対して次にポスチャ検証が試行されるまでの遅延は、NAC Hold Timer 属性（[Configuration] > [VPN] > [NAC]）によって決まります。
N/A	VPN NAC グループ ポリシーに従って NAC がディセーブルになっているピアの数。

表 30-16　show vpn-sessiondb summary コマンド : Active NAC Sessions および Total Cumulative NAC Sessions のフィールド （続き）

フィールド	説明
Non-responsive	ポスチャ検証のための Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP 要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。セキュリティ アプライアンスのコンフィギュレーションがクライアントレス ホストをサポートする場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアのセキュリティ アプライアンスにダウンロードします。クライアントレス ホストをサポートしない場合、セキュリティ アプライアンスは NAC デフォルト ポリシーを割り当てます。
Rejected	ポスチャ検証に失敗したか、または Access Control Server によってアクセス ポリシーが付与されなかったピアの数。

Active VLAN Mapping Sessions テーブルには、ポスチャ検証の対象であるリモート ピアに関する一般的な統計情報が表示されます。

Cumulative VLAN Mapping Sessions テーブルには、ポスチャ検証の対象である、または以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 30-17 に、Active VLAN Mapping Sessions テーブルおよび Cumulative VLAN Mapping Sessions テーブルにあるフィールドの説明を示します。

表 30-17　show vpn-sessiondb summary コマンド : Active VLAN Mapping Sessions および Cumulative Active VLAN Mapping Sessions のフィールド

フィールド	説明
Access	将来的な使用のために予約されています。
Auth	将来的な使用のために予約されています。
Guest	将来的な使用のために予約されています。
N/A	将来的な使用のために予約されています。
Quarantine	将来的な使用のために予約されています。
Static	このフィールドには、事前設定された VLAN に割り当てられている VPN セッションの数が表示されます。

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 wccp

Web Cache Communication Protocol（WCCP）に関連するグローバル統計情報を表示するには、特権 EXEC モードで **show wccp** コマンドを使用します。

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

構文の説明

web-cache	Web キャッシュ サービスの統計情報を指定します。
service-number	（任意）キャッシュが制御する Web キャッシュ サービス グループの ID 番号。指定できる番号の範囲は 0 ～ 256 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。
detail	（任意）ルータおよびすべての Web キャッシュに関する情報を表示します。
view	（任意）特定のサービス グループの他のメンバーが検出されたかどうかを表示します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、WCCP 情報を表示する例を示します。

```
hostname(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                  -not yet determined-
        Protocol Version:                   2.0

    Service Identifier: web-cache
        Number of Cache Engines:            0
        Number of routers:                  0
        Total Packets Redirected:           0
        Redirect access-list:               foo
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  foobar
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
```

```
        Total Bypassed Packets Received:     0
hostname(config)#
```

関連コマンド

コマンド	説明
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

show webvpn csd

CSD がイネーブルかどうかを判定し、イネーブルの場合は実行コンフィギュレーションの CSD バージョンを表示したり、ファイルをテストして有効な CSD 配布パッケージかどうかを確認したりするには、特権 EXEC モードで **show webvpn csd** コマンドを使用します。

show webvpn csd [**image** *filename*]

構文の説明

filename	CSD 配布パッケージとしての有効性をテストするファイルの名前を指定します。この名前は、必ず securedesktop_asa_<*n*>_<*n*>*.pkg の形式とします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

CSD の動作ステータスを確認するには、**show webvpn csd** コマンドを使用します。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `Secure Desktop is not enabled.`

  CSD は実行コンフィギュレーション内にありますが、ディセーブルにされています。CSD をイネーブルにするには、webvpn コンフィギュレーション モードを開始して **csd enable** コマンドを入力します。

- `Secure Desktop version n.n.n.n is currently installed and enabled.`

  CSD はイネーブルに設定されています。バージョン番号は、フラッシュ デバイスから読み込まれる配布パッケージによって決まります。Cisco Secure Desktop Manager には、[ASDM Configuration] > [CSD] のメニュー パスからアクセスできます。ユーザが CSD にアクセスできるのは、CSD コンフィギュレーションに場所が含まれている場合だけです。

ファイルをテストして有効な CSD 配布パッケージかどうかを確認するには、**show webvpn csd image** コマンドを使用します。同様に、webvpn コンフィギュレーション モードで **csd image** コマンドを入力した場合は、コマンドで指定したファイルが有効な CSD 配布パッケージである場合にのみ、CSD がインストールされます。無効なパッケージの場合は、「ERROR: Unable to use CSD image」というメッセージが表示されます。

show webvpn csd image コマンドでファイルをテストして、有効な CSD 配布パッケージかどうかを確認しますが、ファイルが有効な場合でも CSD が自動的にインストールされることはありません。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `ERROR: This is not a valid Secure Desktop image file.`

  ファイル名が securedesktop_asa_<*n*>_<n>*.pkg の形式になっていることを確認します。ファイル名の形式が正しい場合は、次の Web サイトから取得した新しいファイルに置き換えます。

  http://www.cisco.com/cisco/software/navigator.html

  次に、**show webvpn csd image** コマンドを再入力します。イメージが有効な場合は、webvpn コンフィギュレーション モードで **csd image** コマンドおよび **csd enable** コマンドを使用し、CSD をインストールしてイネーブルにします。

- This is a valid Cisco Secure Desktop image:
  Version : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

  ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

例

次に、CSD が実行コンフィギュレーションにインストールされ、イネーブルにされた例を示します。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname#
```

次に、指定したファイルが有効な CSD イメージである例を示します。

```
hostname#show webvpn csd image securedesktop_asa_3_1_0_25.pkg

This is a valid Cisco Secure Desktop image:
  Version  : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

hostname#
```

関連コマンド

コマンド	説明
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

show webvpn group-alias

特定のトンネル グループまたはすべてのトンネル グループのエイリアスを表示するには、特権 EXEC モードで **group-alias** コマンドを使用します。

show webvpn group-alias [*tunnel-group*]

構文の説明

tunnel-group	（任意）グループ エイリアスを表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべてのエイリアスが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1	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 webvpn group-alias コマンドを入力する場合は、WebVPN が実行されている必要があります。

各トンネル グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。

例

次に、トンネル グループ「devtest」のエイリアスを表示する **show webvpn group-alias** コマンドと、このコマンドの出力例を示します。

```
hostname# show webvpn group-alias devtest
QA
Fra-QA
```

関連コマンド

コマンド	説明
group-alias	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn group-url

特定のトンネル グループまたはすべてのトンネル グループの URL を表示するには、特権 EXEC モードで **group-url** コマンドを使用します。

show webvpn group-url [*tunnel-group*]

構文の説明

tunnel-group	（任意）URL を表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名が入力されなかった場合は、すべてのトンネル グループのすべての URL が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	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 webvpn group-url コマンドを入力する場合は、WebVPN が実行されている必要があります。各グループには複数の URL があることも、URL がまったくないこともあります。

例

次に、トンネル グループ「frn-eng1」の URL を表示する **show webvpn group-url** コマンドと、このコマンドの出力例を示します。

```
hostname# show webvpn group-url
http://www.cisco.com
https://fra1.vpn.com
https://fra2.vpn.com
```

関連コマンド

コマンド	説明
group-url	グループに対して 1 つ以上の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

show webvpn sso-server

WebVPN シングル サインオン サーバに関する運用統計情報を表示するには、特権 EXEC モードで **show webvpn sso-server** コマンドを使用します。

show webvpn sso-server [*name***]**

構文の説明

name	（任意）SSO サーバの名前を指定します。サーバ名の長さは 4 ～ 31 文字にする必要があります。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**show webvpn sso-server** コマンドは、セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。

SSO サーバ名引数が入力されていない場合は、すべての SSO サーバの統計情報が表示されます。

例

次に、特権 EXEC モードでコマンドを入力し、タイプが SiteMinder、名前が example である SSO サーバの統計情報を表示する例を示します。

```
hostname# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
```

```
Number of unrecognized responses:  0
hostname#
```

次に、特定の SSO サーバ名を指定せずにこのコマンドを発行することで、セキュリティ アプライアンスで設定されているすべての SSO サーバに関する統計情報を表示する例を示します。

```
hostname#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
asa1(config-webvpn)#
```

関連コマンド

コマンド	説明
max-retry-attempts	セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

show webvpn svc

セキュリティ アプライアンスにインストールされ、キャッシュ メモリに読み込まれる SSL VPN クライアント イメージについての情報を表示するには、またはファイルが有効なクライアント イメージであるかテストするには、特権 EXEC モードで **show webvpn svc** コマンドを使用します。

show webvpn svc [**image** *filename*]

構文の説明

image *filename*	SSL VPN クライアント イメージ ファイルとしてテストするファイルの名前を指定します。

デフォルト

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシュ メモリにロードされ、リモート PC にダウンロード可能な SSL VPN クライアント イメージに関する情報を表示するには、**show webvpn svc** コマンドを使用します。ファイルをテストして有効なイメージかどうかを確認するには、**image** *filename* のキーワードと引数を使用します。ファイルが有効なイメージではない場合、次のメッセージが表示されます。

```
ERROR: This is not a valid SSL VPN Client image file.
```

例

次に、現在インストールされているイメージに対する **show webvpn svc** コマンドの出力例を示します。

```
hostname# show webvpn svc
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

次に、有効なイメージに対する **show webvpn svc image** *filename* コマンドの出力例を示します。

```
F1(config-webvpn)# show webvpn svc image sslclient-win-1.0.2.127.pkg
```

```
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

関連コマンド

コマンド	説明
svc enable	セキュリティ アプライアンスで SSL VPN クライアントをリモート PC にダウンロードできるようにします。
svc image	セキュリティ アプライアンスがフラッシュ メモリからキャッシュメモリに SSL VPN クライアント ファイルをロードするようにします。クライアント イメージをオペレーティング システムと照合するときに、セキュリティ アプライアンスがクライアント イメージの各部分をリモート PC にダウンロードする順序を指定します。
vpn-tunnel-protocol	SSL VPN クライアントが使用する SSL を含め、リモート VPN ユーザの特定の VPN トンネル プロトコルをイネーブルにします。

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

構文の説明

count	変換数を表示します。
debug	（任意）xlate の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）グローバル IP アドレスまたはアドレス範囲を指定して、アクティブな変換を表示します。
gport *port1*[*-port2*]	グローバル ポートまたはポート範囲を指定して、アクティブな変換を表示します。
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）ローカル IP アドレスまたはアドレス範囲を指定して、アクティブな変換を表示します。
lport *port1*[*-port2*]	ローカル ポートまたはポート範囲を指定して、アクティブな変換を表示します。
netmask *mask*	（任意）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*	（任意）状態を指定して、アクティブな変換を表示します。次の 1 つ以上の状態を入力できます。 • **static**：スタティック変換を指定します。 • **portmap**：PAT グローバル変換を指定します。 • **norandomseq**：**norondomseq** 設定での **nat** または**スタティック**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、状態をスペースで区切ってください。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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 30-18 に、変換フラグの定義を示します。

表 30-18　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 A RR リライト
I	**nat 0** からの ID 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複数の xlate が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 つのアクティブな PAT とともに変換スロット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。3 つのアクティブな PAT とともに、変換タイプおよびインターフェイス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 - dynamic, 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。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 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クリアします。
show conn	すべてのアクティブ接続を表示します。
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	現在認証済みのユーザを表示します。