CHAPTER 30

show service-policy コマンド～ show webvpn svc コマンド

show service-policy

設定済みのサービス ポリシーを表示するには、グローバル コンフィギュレーション モードで ***show service-policy*** コマンドを使用します。

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

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*]]

シンタックスの説明

csc	（オプション）***csc*** コマンドを含んでいるポリシーだけを出力します。
dest_ip	トラフィック フローの宛先 IP アドレス。
dest_mask	トラフィック フローの宛先 IP アドレスのサブネット マスク。
dest_port	（オプション）トラフィック フローで使用されている宛先ポート。
details	（オプション）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制限情報を表示します。
eq	（オプション）等号。送信元または宛先のポートが、以降に指定するポート番号と一致することを要求します。
flow	（オプション）セキュリティ アプライアンスでポリシーの適用対象となるトラフィック フローを指定します。このフローに適用されるポリシーが表示されます。***flow*** キーワードに続いて指定する引数とキーワードでは、フローを IP 5 タプル形式で指定します。
global	（オプション）すべてのインターフェイスに適用されるグローバル ポリシーのみを出力します。
host *dest_host*	トラフィック フローの宛先ホストの IP アドレス。
host *src_host*	トラフィック フローの送信元ホストの IP アドレス。
icmp_control_message	（オプション）トラフィック フローの ICMP 制御メッセージを指定します。*icmp_control_message* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
icmp_number	（オプション）トラフィック フローの ICMP プロトコル番号を指定します。
inspect	（オプション）**inspect** コマンドを含んでいるポリシーだけを出力します。

interface *intf*	（オプション）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* は、**nameif** コマンドで定義したインターフェイス名です。
ips	**ips** コマンドを含んでいるポリシーだけを出力します。
police	**police** コマンドを含んでいるポリシーだけを出力します。
priority	**priority** コマンドを含んでいるポリシーだけを出力します。
set connection	**set connection** コマンドを含んでいるポリシーだけを出力します。
protocol	トラフィック フローで使用されているプロトコル。*protocol* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
src_ip	トラフィック フローで使用されている送信元 IP アドレス。
src_mask	トラフィック フローで使用されている送信元 IP ネットマスク。
src_port	トラフィック フローで使用されている送信元ポート。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが ***csc*** キーワードを追加するように変更されました。

使用上のガイドライン

flow キーワードを使用すると、記述可能な任意のフローについて、セキュリティ アプライアンスがそのフローに適用するポリシーを特定できます。この情報を利用すると、必要なサービスがこのサービス ポリシー コンフィギュレーションによって特定の接続に提供されるかどうかを確認できます。***flow*** キーワード以降に指定する引数とキーワードでは、オブジェクト グループ化をしていないフローを IP 5 タプル形式で指定します。

フローを IP 5 タプル形式で記述するため、すべての一致基準がサポートされるわけではありません。次に、フローの検索でサポートされている一致基準のリストを示します。

- ***match access-list***
- ***match port***
- ***match rtp***
- ***match default-inspection-traffic***

priority キーワードは、インターフェイスを経由して転送されたパケットの集約カウンタ値を表示するために使用します。

show service-policy コマンドの出力に表示される初期接続の数は、**class-map** コマンドで定義したトラフィック マッチングと一致したインターフェイスに向かう現在の初期接続の数を示しています。`embryonic-conn-max` フィールドは、モジュラ ポリシー フレームワークを使用するトラフィック クラスに対して設定した最大初期接続数の制限値を示しています。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続が **class-map** コマンドで定義したトラフィック タイプと一致すると、その接続に対して TCP 代行受信が適用されます。

protocol 引数の値

次に、*protocol* 引数で有効となる値を示します。

- *number*：プロトコル番号（0 ～ 255）
- ***ah***
- ***eigrp***
- ***esp***
- ***gre***
- ***icmp***
- ***icmp6***
- ***igmp***
- ***igrp***
- ***ip***
- ***ipinip***
- ***ipsec***
- ***nos***
- ***ospf***
- ***pcp***
- ***pim***
- ***pptp***
- ***snp***
- ***tcp***
- ***udp***

icmp_control_message 引数の値

次に、*icmp_control_message* 引数で有効となる値を示します。

- ***alternate-address***
- ***conversion-error***
- ***echo***
- ***echo-reply***
- ***information-reply***
- ***information-request***
- ***mask-reply***
- ***mask-request***
- ***mobile-redirect***
- ***parameter-problem***
- ***redirect***
- ***router-advertisement***
- ***router-solicitation***
- ***source-quench***
- ***time-exceeded***
- ***timestamp-reply***
- ***timestamp-request***
- ***traceroute***

- *unreachable*

例

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

```
hostname# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
hostname# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap


hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq
5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。
clear service-policy	すべてのサービス ポリシーのコンフィギュレーションを消去します。
service-policy	サービス ポリシーを設定します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show service-policy inspect gtp

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

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | ***pdpmcb*** | **requests** | **statistics** [**gsn** *IP_address*] }

シンタックスの説明

apn	（オプション）指定した APN に基づいて、PDP コンテキストの詳細な出力を表示します。
ap_name	統計情報を表示する特定のアクセス ポイント名を指定します。
detail	（オプション）PDP コンテキストの詳細な出力を表示します。
imsi	指定した IMSI に基づいて、PDP コンテキストの詳細な出力を表示します。
IMSI_value	統計情報を表示する特定の IMSI を指定するための 16 進値。
interface	（オプション）特定のインターフェイスを指定します。
int	情報を表示するインターフェイスを指定します。
gsn	（オプション）GPRS サポート ノードを指定します。このノードは、GPRS 無線データ ネットワークとその他のネットワークの間にあるインターフェイスです。
gtp	（オプション）GTP のサービス ポリシーを表示します。
IP_address	統計情報を表示する IP アドレス。
ms-addr	（オプション）指定したモバイル ステーション（MS）アドレスに基づいて、PDP コンテキストの詳細な出力を表示します。
pdp-context	（オプション）パケット データ プロトコル コンテキストを指定します。
pdpmcb	（オプション）PDP マスター制御ブロックのステータスを表示します。
requests	（オプション）GTP 要求のステータスを表示します。
statistics	（オプション）GTP 統計情報を表示します。
tid	（オプション）指定した TID に基づいて、PDP コンテキストの詳細な出力を表示します。
tunnel_ID	統計情報を表示する特定のトンネルを指定するための 16 進値。
version	（オプション）GTP バージョンに基づいて、PDP コンテキストの詳細な出力を表示します。
version_num	統計情報を表示する PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

縦線（|）を使用すると、表示内容をフィルタリングできます。表示フィルタリング オプションの詳細については、| を入力してください。

show pdp-context コマンドは、PDP コンテキストに関する情報を表示します。

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合せであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション ユーザの間で転送するために必要なものです。

show gtp requests コマンドは、要求キューに入っている現在の要求を表示します。

例

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

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦線（|）を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次のコマンドでは、GTP 検査の統計情報を表示しています。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次のコマンドでは、PDP コンテキストに関する情報を表示しています。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 30-1 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各カラムの説明を示します。

表 30-1　PDP コンテキスト

カラムのヘッダー	説明
Version	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr	サービス提供ゲートウェイ サービス ノードを表示します。
Idle	PDP コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。

show service-policy inspect radius-accounting

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 radius-accounting** コマンドを使用します。

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

シンタックスの説明

interface *int*	（オプション）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

次の表は、このコマンドを入力できるモードを示しています。

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

例

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

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦線（|）を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次のコマンドでは、GTP 検査の統計情報を表示しています。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次のコマンドでは、PDP コンテキストに関する情報を表示しています。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 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カラムの説明を示します。

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先のトラフィック クラスを定義します。

show shun

排除情報を表示するには、特権 EXEC モードで **show shun** コマンドを使用します。

show shun [*src_ip* | *statistics*]

シンタックスの説明

src_ip	（オプション）このアドレスに関する情報を表示します。
statistics	（オプション）インターフェイスのカウンタのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show shun** コマンドの出力例を示します。

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
shun	新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにします。

show sip

SIP セッションを表示するには、特権 EXEC モードで **show sip** コマンドを使用します。

show sip

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show sip** コマンドは、SIP 検査エンジンの問題のトラブルシューティングに役立ちます。説明は、**inspect protocol sip udp 5060** コマンドと一緒にします。**show timeout sip** コマンドは、指示されているプロトコルのタイムアウト値を表示します。

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

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

例　次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

この例は、セキュリティ アプライアンス上の 2 つのアクティブな SIP セッションを示しています（`Total` フィールドで示されているように）。各 `call-id` は、コールを表わしています。

最初のセッションは、call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションはまだコール セットアップ中であることを示しています。コール セットアップが完了するのは、ACK が確認されたときのみです。このセッションは、1 秒間アイドル状態でした。

2 番目のセッションは、Active 状態です。ここでは、コール セットアップは完了して、エンドポイントはメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug sip	SIP のデバッグ情報をイネーブルにします。
inspect sip	SIP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show skinny

SCCP（Skinny）検査エンジンの問題をトラブルシューティングするには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）検査エンジンの問題のトラブルシューティングに役立ちます。

例

次の条件での **show skinny** コマンドの出力例を示します。セキュリティ アプライアンスを越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
hostname# show skinny

        LOCAL                   FOREIGN                 STATE

-----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力は、両方の内部 Cisco IP Phone 間でコールが確立されていることを示します。最初と 2 番目の電話機の RTP リスニング ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D | DNS, d | dump, I | identity, i | inside, n | no random,
 | o | outside, r | portmap, s | static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show sla monitor configuration

SLA オペレーションのデフォルトを含む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*]

シンタックスの説明

sla-id	（オプション）SLA オペレーションの 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、すべての SLA オペレーション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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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 オペレーション 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** コマンドの出力例を示します。SLA オペレーション 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 オペレーションの **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 オペレーション コンフィギュレーション コマンドを表示します。
sla monitor	SLA 監視オペレーションを定義します。

show sla monitor operational-state

SLA オペレーションの操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*]

シンタックスの説明

sla-id	（オプション）SLA オペレーションの 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、すべての SLA オペレーションの統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 オペレーション 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 オペレーション コンフィギュレーション コマンドを表示します。
sla monitor	SLA 監視オペレーションを定義します。

show snmp-server statistics

SNMP サーバに関する統計情報を表示するには、特権 EXEC モードで **show snmp-server statistics** コマンドを使用します。

show snmp-server statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

この例は、SNMP サーバ統計情報を表示する方法を示しています。

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
clear configure snmp-server	簡易ネットワーク管理プロトコル(SNMP)サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバのコンフィギュレーションを表示します。

show ssh sessions

セキュリティ アプライアンス上のアクティブな SSH セッションの情報を表示するには、特権 EXEC モードで **show ssh sessions** コマンドを使用します。

show ssh *sessions* [*ip_address*]

シンタックスの説明

ip_address	（オプション）指定した IP アドレスのセッション情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

SID は、SSH セッションを識別する一意な番号です。Client IP は、SSH クライアントを実行しているシステムの IP アドレスです。Version は、SSH クライアントがサポートしているプロトコル バージョン番号です。SSH が SSH バージョン 1 のみサポートしている場合、Version カラムには 1.5 が表示されます。SSH クライアントが SSH バージョン 1 と SSH バージョン 2 の両方をサポートしている場合、Version カラムには 1.99 が表示されます。SSH クライアントが SSH バージョン 2 のみサポートしている場合、Version カラムには 2.0 が表示されます。Encryption カラムには、SSH クライアントが使用している暗号化のタイプが表示されます。State カラムには、クライアントとセキュリティ アプライアンスとの対話の進行状況が表示されます。Username カラムには、セッションで認証されているログイン ユーザ名が表示されます。

例

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

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

関連コマンド

コマンド	説明
ssh disconnect	アクティブな SSH セッションを切断します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

show startup-config

スタートアップ コンフィギュレーションを表示するか、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するには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [errors]

シンタックスの説明

errors	（オプション）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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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、シングルモードで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、このコマンドは現在の実行スペース（システム コンフィギュレーションまたはセキュリティ コンテキスト）のスタートアップ コンフィギュレーションを表示します。

メモリからスタートアップ エラーを消去するには、**clear startup-config errors** コマンドを使用します。

例

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

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.0(0)28
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

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

```
hostname# show startup-config errors

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

関連コマンド

コマンド	説明
clear startup-config errors	メモリからスタートアップ エラーを消去します。
show running-config	実行コンフィギュレーションを表示します。

show sunrpc-server active

Sun RPC サービス用に開いているピンホールを表示するには、特権 EXEC モードで **show sunrpc-server active** コマンドを使用します。

show sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show sunrpc-server active コマンドは、NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するために使用します。

例

Sun RPC サービス用に開いているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールを消去します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	Sun RPC サービスのコンフィギュレーションに関する情報を表示します。

show switch mac-address-table

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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 テーブルでは、スイッチ ハードウェアの各 VLAN 内にトラフィック用の MAC アドレス対スイッチ ポートのマッピングが維持されます。透過ファイアウォール モードの場合、**show mac-address-table** コマンドを使用して ASA ソフトウェアのブリッジ MAC アドレス テーブルを表示します。ブリッジ MAC アドレス テーブルでは、VLAN 間を通過するトラフィック用の MAC アドレス対 VLAN のインターフェイス マッピングが維持されます。

MAC アドレス エントリは 5 分間で無効になります。

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 アドレスが、スタティック マルチキャスト アドレスとしてダイナミックにラーニングされたか、スタティックにラーニングされたかを示します。内部バックプレーン インターフェイスの場合にのみスタティック エントリになります。
Age	MAC アドレス テーブルにダイナミック エントリの経過時間を表示します。
:port	MAC アドレスを持つ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	組み込みスイッチを持たないモデルの 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

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、特権 EXEC モードで **show switch vlan** コマンドを使用して VLAN と、関連付けられたスイッチ ポートを表示します。

show switch vlan

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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。他のモデルでは、**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。名前が **nameif** コマンドを使用して設定されていない場合、または **interface vlan** コマンドがない場合、ダッシュ（-）が表示されます。
Status	up ステータスまたは down ステータスで、スイッチの VLAN からトラフィックを受信するか、スイッチの VLAN にトラフィックを送信するかを示します。VLAN が up ステータスになるには、VLAN のスイッチ ポートが最低でも 1 つ up 状態でなければなりません。
:port	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 についてリストされている場合、そのスイッチ ポートはトランク ポートです。上記の出力例は、Ethernet 0/1 が VLAN 100 および 300 を伝送するトランク ポートであることを示します。

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消去します。
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 モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show vlan	組み込みスイッチを持たないモデルの 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 アドレスと IPv6 アドレスをサポートしています。

show tcpstat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを表示できます。表 30-5 は、表示される TCP 統計情報を説明しています。

表 30-5　show tcpstat コマンドでの TCP 統計情報

統計情報	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可によって使用されます。
tcp_xmt pkts	TCP スタックによって送信されたパケットの数。
tcp_rcv good pkts	TCP スタックによって受信された正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	不良チェックサムを保持していた受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザを追加しようとしたときに、ユーザがすでにハッシュ テーブル内に存在していた回数。
tcp user srch hash hit	検索時に TCP ユーザがハッシュ テーブル内で検出された回数。
tcp user srch hash miss	検索時に TCP ユーザがハッシュ テーブル内で検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたときに、ユーザがハッシュ テーブル内で検出されなかった回数。

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

統計情報	説明
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態（RFC 793 を参照）。表示される値を次に示します。 1　CLOSED 2　LISTEN 3　SYN_SENT 4　SYN_RCVD 5　ESTABLISHED 6　FIN_WAIT_1 7　FIN_WAIT_2 8　CLOSE_WAIT 9　CLOSING 10　LAST_ACK 11　TIME_WAIT
rexqlen	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値（ミリ秒）。
to_timer	TCP ユーザの非活動タイムアウト タイマーの値（ミリ秒）。
cl_timer	TCP ユーザのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザの持続タイマーの値（ミリ秒）。
rt_timer	TCP ユーザの再送信タイマーの値（ミリ秒）。
tries	TCP ユーザの再送信カウント。

例

次の例は、セキュリティ アプライアンスの TCP スタックのステータスを表示する方法を示しています。

```
hostname# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [**detail** | **file** | **no-config**]

シンタックスの説明

detail	（オプション）詳細情報を表示します。
file	（オプション）コマンドの出力をファイルに書き込みます。
no-config	（オプション）実行コンフィギュレーションの出力を除外します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	***detail*** キーワードと ***file*** キーワードが追加されました。
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。**show** コマンドからの出力を組み合せて、テクニカル サポート アナリストに対して最も多くの情報を提供します。

例

次の例は、テクニカル サポートで分析に使用する情報を、実行コンフィギュレーションの出力を除外して表示する方法を示しています。

```
hostname# show tech-support no-config

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

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

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

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
```

```
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

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

00:08:14.911 UTC Sun Apr 17 2005

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

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

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

0 in use, 0 most used

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

0 in use, 0 most used

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

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

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

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
```

```
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

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

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

------------------ show 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 Server（PFSS）と公開キー インフラストラクチャ（PKI）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータス、およびどのセキュリティ アプライアンスがアクティブになっているかを表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	セキュリティ アプライアンスのパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	セキュリティ アプライアンス上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show track

トラッキング プロセスにより追跡され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*]

シンタックスの説明

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 が提供されない場合、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

次の表は、このコマンドを入力できるモードを示しています。

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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）。このコマンドが入力されていた場合、この秒数は、コマンドが入力された時点からの経過時間です。

ASA 5550 適応型セキュリティ アプライアンスの場合、**show traffic** コマンドはスロットごとの集約スループットも表示します。ASA 5550 適応型セキュリティ アプライアンスではスループットを最大限にするためにトラフィックが均一に配布されることが求められますが、この集約スループットの表示により、トラフィックが均一に配布されていることを簡単に判別できます。

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

現在認証されている 1 人またはすべてのユーザ、ユーザがバインドされているホスト IP、キャッシュされた IP およびポート認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

show uauth [*username*]

シンタックスの説明

username	（オプション）表示するユーザ認証情報とユーザ認可情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認可情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

timeout コマンドと共に使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。ユーザ ホストごとにアドレスとサービスのペアを最大 16 個までキャッシュできます。ユーザが適切なホストから、キャッシュされたサービスにアクセスしようとすると、セキュリティ アプライアンスはユーザを認可済みであると見なし、すぐに接続を代理処理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、各イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。このプロセスにより、認可サーバ上でパフォーマンスが大幅に向上し、負荷も大幅に軽減されます。

show uauth コマンドの出力では、認証および認可の目的で認可サーバに提供されたユーザ名が表示されます。また、ユーザ名がバインドされている IP アドレス、ユーザが認証されただけであるか、キャッシュされたサービスを持っているかが表示されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能と共に 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 エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドの項を参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザが認証されておらず、1 人のユーザの認証が進行中である場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

次に、3 人のユーザが認証され、セキュリティ アプライアンスを介してサービスを使用することを認可されている場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

関連コマンド

コマンド	説明
clear uauth	現在のユーザの認証情報と認可情報を削除します。
timeout	アイドル状態の最大継続時間を設定します。

show url-block

url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（ある場合）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

show url-block [**block statistics**]

シンタックスの説明

block statistics	（オプション）ブロック バッファ使用状況の統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show url-block block statistics コマンドは、url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（ある場合）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 バッファ使用状況カウンタを消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
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 フィルタリング サーバまたは Websense フィルタリング サーバから受信された URL 応答に使用される、URL キャッシュに関する情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

show url-cache statistics

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show url-cache statistics** コマンドは、次のエントリを表示します。

- Size：KB 単位で表したキャッシュ サイズ。**url-cache** *size* オプションを使用して設定します。
- Entries：キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use：現在キャッシュにあるエントリ数。
- Lookups：セキュリティ アプライアンスがキャッシュ エントリを検索した回数。
- Hits：セキュリティ アプライアンスがキャッシュ内でエントリを検出した回数。

show perfmon コマンドを使用して、N2H2 Sentian または Websense フィルタリング アクティビティに関する追加情報を表示できます。

例

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

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 | Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 | Hits :     290
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバ ベンダー、URL の合計数、許可された数、拒否された数、HTTPS 接続の合計数、許可された数、拒否された数、TCP 接続の合計数、許可された数、拒否された数、および URL サーバ ステータスを表示します。

show url-server コマンドは、次の情報を表示します。

- N2H2 の場合 : **url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- Websense の場合 : **url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

例

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

```
hostname## show url-server statistics
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消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
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 コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示するには、特権 EXEC モードで **show version** コマンドを使用します。

show version

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	ステートフル フェールオーバー モードでは、クラスタの稼働時間を示す行が表示されるように変更されました。

使用上のガイドライン　**show version** コマンドを使用すると、ソフトウェア バージョン、最後にリブートされて以降の動作時間、プロセッサ タイプ、フラッシュ パーティション タイプ、インターフェイス ボード、シリアル番号（BIOS ID）、アクティベーション キー値、ライセンス タイプ（R または UR）、および、コンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

show version コマンドで表示されるシリアル番号は、フラッシュ パーティション BIOS のものです。シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを取得する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

（注）　稼働時間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台の装置が動作を停止した場合、他の装置が動作を継続している限り、稼働時間の値は増加していきます。

例

次の例は、ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンスキー、および関連する稼働時間データを表示する方法を示しています。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 クラスタの稼働時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 PIX Security Appliance Software Version 7.0(4)
Device Manager Version 5.0(4)

Compiled on Tue 27-Sep-05 10:41 by root
System image file is "flash:/cdisk.bin"
Config file at boot was "startup-config"

pix2 up 7 days 7 hours
failover cluster up 2 mins 44 secs


Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 0: Ext: Ethernet0           : address is 0011.2094.1d2b, irq 10
 1: Ext: Ethernet1           : address is 0011.2094.1d2c, irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Enabled
VPN Peers                   : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: 808184143
Running Activation Key: 0xcf22f25d 0xec1c3174 0x8cb138a0 0xaad8b878 0x4f32fd90
Configuration last modified by enable_15 at 14:18:26.103 UTC Thu Oct 6 2005
hostname#
```

関連コマンド

コマンド	説明
show hardware	ハードウェアの詳細情報を表示します。
show serial	ハードウェアのシリアル情報を表示します。
show uptime	セキュリティ アプライアンスが動作している期間の長さを表示します。

show 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

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、設定されている VLAN を表示します。

```
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消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show vpn load-balancing

VPN ロードバランシング仮想クラスタのコンフィギュレーションに関する実行時統計情報を表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロードバランシング モードで **show vpn load-balancing** コマンドを使用します。

show vpn load-balancing

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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 カラムおよび SSL カラムが追加されました。

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、このデバイスには VPN ロードバランシングが設定されていないことを通知します。

出力のアスタリスク（*）は、接続しているセキュリティ アプライアンスの IP アドレスを示します。

例

次の例は、ローカル デバイスが VPN ロードバランシング クラスタに参加している場合の **show vpn load-balancing** コマンドおよびその出力を示しています。

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
                                          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)#
```

ローカル デバイスが VPN ロードバランシング クラスタに参加していない場合、**show vpn load-balancing** コマンドは、上とは異なる次のような結果を表示します。

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド文を削除します。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

show vpn-sessiondb

VPN セッションに関する情報を表示するには、特権 EXEC モードで **show vpn-sessiondb** コマンドを使用します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できるほか、情報をフィルタリングおよびソートするためのオプションが用意されています。「シンタックスの説明」の表と「使用上のガイドライン」で、それぞれの使用可能なオプションについて説明しています。

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

シンタックスの説明

表示の詳細度	
detail	セッションに関する詳細な情報を表示します。たとえば、IPSec セッションに対して **detail** オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの追加の詳細情報が表示されます。 **detail** と **full** オプションを指定すると、セキュリティ アプライアンスはマシンで読み取り可能な形式で詳細出力を表示します。
filter	1 つ以上のフィルタ オプションを使用して、指定する情報のみを表示するように出力をフィルタリングします。詳細については、使用上の注意を参照してください。
full	連続した、短縮されていない出力を表示します。出力の各レコード間は、| 記号と || 文字列で区切られます。
sort	指定するソート オプションに従って出力をソートします。詳細については、使用上の注意を参照してください。
表示するセッション タイプ	
email-proxy	電子メールプロキシ セッションを表示します。電子メールプロキシ セッションに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**（接続名）、**ipaddress**（クライアント）、**encryption** を使用して情報をフィルタリングすることもできます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号（1 ～ 750）を指定します。フィルタ オプションとソート オプションは適用されません。
l2l	VPN の LAN-to-LAN セッション情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
remote	リモートアクセス セッションを表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションである **name**、**a-ipaddress**、**p-ipaddress**、**tunnel-group**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
webvpn	WebVPN セッションに関する情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**encryption** を使用して情報をフィルタリングすることもできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	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　次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ / ソート オプション	意味
filter a-ipaddress *IPaddr*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）についてのみ情報を表示します。
sort a-ipaddress	割り当て済み IP アドレスを基準として、表示内容をソートします。
filter encryption *encryption-algo*	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションについてのみ情報を表示します。
sort encryption	暗号化アルゴリズムを基準として、表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
filter ipadddress *IPaddr*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）についてのみ情報を表示します。
sort ipaddress	内部 IP アドレスを基準として、表示内容をソートします。
filter name *username*	出力をフィルタリングして、指定したユーザ名（複数可）に関するセッションを表示します。
sort name	ユーザ名を基準として、表示内容をアルファベット順でソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスについてのみ情報を表示します。
sort p-address	指定した外部 IP アドレス（複数可）を基準として、表示内容をソートします。
filter protocol *protocol-name*	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションについてのみ情報を表示します。
sort protocol	プロトコルを基準として、表示内容をソートします。プロトコルには、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）についてのみ情報を表示します。
sort tunnel-group	トンネル グループを基準として、表示内容をソートします。

フィルタ / ソート オプション	意味
| 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: 1 | Username: dbrownhi | Tunnel Group: bxbvpnlab | IP Addr: 192.168.2.70 |
Public IP: 10.86.5.114 | Protocol: IPSec | Encryption: AES128 | Login Time: 15:22:46
EDT Tue May 10 2005 |Duration: 6h:57m:40s | Bytes Tx: 0 | Bytes Rx: 598357 | Client
Type: WinNT | Client Ver: 4.6.00.0049 | Filter Name: | NAC Result: Accepted | Posture
Token: Healthy ||

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

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeysXauth | UDP Source Port:
500 | UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES
| Hashing: MD5 | Diffie-Hellman Group: 2 | Rekey Time Interval: 86400 Seconds| Rekey
Left(T): 61341 Seconds ||

Type: IPSec | Session ID: 2 | Local IP Addr: 0.0.0.0 | Remote IP Addr: 192.168.2.70 |
Encryption: AES128 | Hashing: SHA1 | Encapsulation: Tunnel | Rekey Time Interval:
28800 Seconds | Rekey Left(T): 26794 Seconds | Bytes Tx: 0 | Bytes Rx: 598357 |
Packets Tx: 0 | Packets Rx: 8044 | ||

Type: NAC | Revalidation Time Interval: 3000 Seconds | Time Until Next Revalidation:
286 Seconds | Status Query Time Interval: 600 Seconds | EAPoUDP Session Age: 2714
Seconds | Hold-Off Time Remaining: 0 Seconds | Posture Token: Healthy | Redirect URL:
www.cisco.com ||

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

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
```

例に示されているように、**show vpn-sessiondb** コマンドに応答して表示されるフィールドは、入力するキーワードにより異なります。表 30-6 では、これらのフィールドについて説明しています。

表 30-6　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 アプライアンスにより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 アプライアンスによりリモートのピアまたはクライアントへ送信されたバイト数。
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（可能な場合）。
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とキー サイズ。
Duration	セッション 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 ESP（カプセル化セキュリティ 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（存在する場合）。
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で、IPSec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining の略です。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）。
IKE Sessions	IKE（IPSec フェーズ 1）セッションの数で、通常は 1 です。これらのセッションは IPSec トラフィックのトンネルを確立します。
Index	このレコードの一意の ID。
IP Addr	このセッション用にリモート 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 IP アドレスまたは仮想 IP アドレスとも呼ばれます。このアドレスにより、クライアントはプライベート ネットワークでホストと見なされます。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
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 ポスチャ確認の状態。状態は次のいずれかになります。 • Accepted：ACS は正常にリモート ホストのポスチャを確認しました。 • Rejected：ACS はリモート ホストの確認に失敗しました。 • Exempted：セキュリティ アプライアンスで設定されたポスチャ確認免除リストに従い、リモート ホストはポスチャ確認を免除されました。 • 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：セキュリティ アプライアンスで、ポスチャ確認に成功した後、リモート ホストと EAPoUDP の通信が途絶えました。 • N/A：NAC は VPN NAC グループ ポリシーに応じてリモート ホストに対してディセーブルになります。 • Unknown：ポスチャ確認が進行中です。
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 アプライアンスによりリモート ピアから受信したパケット数。
Packets Tx	セキュリティ アプライアンスによりリモート ピアに送信されたパケット数。
PFS Group	完全転送秘密グループ数。
Posture Token	アクセス コントロール サーバ上で設定可能な情報テキスト文字列。ACS は、ポスチャ トークンを情報提供の目的でセキュリティ アプライアンスにダウンロードし、システムのモニタリング、レポート、デバッグ、およびロギングに使用します。通常のポスチャ 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、パブリックにルーティング可能な IP アドレス。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Redirect URL	ポスチャ確認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）要求と 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 要求と 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、ポスチャ確認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 Redirect URL に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 暗号キーの残り有効期限。
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 エンドポイントに割り当てられた IP アドレス（リモート ピア上のインターフェイス）。
Reval Int (T)	Revalidation Time Interval の略です。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 の略です。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 秒です。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 の略です。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 秒です。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	アトリビュート値を求めるために、このトンネルが参照するトンネル グループ名。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
UDP Dst Port または UDP Destination Port	UDP についてリモート ピアが使用するポート番号。
UDP Src Port または UDP Source Port	UDP についてセキュリティ アプライアンスが使用するポート番号。
Username	セッションを確立するために使用したユーザのログイン名。

関連コマンド

コマンド	説明
show running-configuration vpn-sessiondb	VPN セッション データベースの実行コンフィギュレーションを表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。
show vpn-sessiondb summary	すべての VPN セッションの要約を表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルまたは暗号化アルゴリズムごとの比率（%）を表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

シンタックスの説明

encryption	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化について指定します。暗号化アルゴリズムには、次の種類があります。 aes128　des aes192　3des aes256　rc4
filter *groupname*	出力をフィルタリングして、指定するトンネル グループについてのみセッション比率を表示します。
protocol	表示するプロトコルを指定します。プロトコルには、次の種類があります。 IKE　SMTPS IMAP4S　userHTTPS IPSec　vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**encryption** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio enc
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions        Percent
none                     0                0%
DES                      1               20%
3DES                     0                0%
AES128                   4        80%
AES192                   0                0%
AES256                   0                0%
```

次に、**protocol** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions        Percent
IKE                      0                0%
IPSec                    1               20%
IPSecLAN2LAN             0                0%
IPSecLAN2LANOverNatT     0                0%
IPSecOverNatT            0                0%
IPSecOverTCP             1 20%
IPSecOverUDP             0                0%
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 セッション、WebVPN セッション、およびネットワーク アドミッション コントロール セッションの要約を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	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 vpn-sessiondb summary** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb summary

Active Sessions:                          Session Information:
  IPSec LAN-to-LAN       : 0                  Peak Concurrent        : 0
  IPSec Remote Access    : 0                  IPSec Limit            : 750
  WebVPN                 : 0                  WebVPN Limit           : 500
  SSL VPN Client (SVC)   : 0                  Cumulative Sessions    : 0
  Email Proxy            : 0
  Total Active Sessions  : 0                  Percent Session Load   : 0%
                                              VPN LB Mgmt Sessions   : 0

Active NAC Sessions:                      Cumulative NAC Sessions:
  Accepted               : 0                  Accepted               : 0
  Rejected               : 0                  Rejected               : 0
  Exempted               : 0                  Exempted               : 0
  Non-responsive         : 0                  Non-responsive         : 0
  Hold-off               : 0                  Hold-off               : 0
  N/A                    : 0                  N/A                    : 0
F1-asa1#
```

セッションとは、特定のピアで確立された VPN トンネルです。IPSec LAN-to-LAN トンネルは 1 つのセッションとしてカウントされ、トンネル経由で多くのホスト間接続が許可されます。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 つのリモート アクセス トンネルです。

表 30-7 では、アクティブ セッション テーブルとセッション情報テーブルのフィールドを説明します。

表 30-7　show vpn-sessiondb summary コマンド:アクティブ セッションとセッション情報のフィールド

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ブートまたはリセットされてから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 セッション数。
Peak Concurrent	セキュリティ アプライアンスが最後にブートまたはリセットされてから、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 を使用可能なセッションの最大数で割った値に等しく、パーセンテージで表示されます。使用可能なセッションの最大数は、次のいずれかの値です。 • ライセンスがある IPSec セッションと WebVPN 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、IPSec through NAT セッション数。
Total Active Sessions	現在アクティブなすべてのタイプのセッション数。

アクティブな NAC セッション テーブルには、ポスチャ確認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。

NAC 累積セッション テーブルには、ポスチャ確認の対象である、あるい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 30-8 では、アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールドについて説明します。

表 30-8　show vpn-sessiondb summary コマンド : アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールド

フィールド	説明
Accepted	ポスチャ確認が成功し、アクセス コントロール サーバによりアクセス ポリシーが供与されたピアの数。
Exempted	セキュリティ アプライアンス上で設定されたポスチャ確認免除リストのエントリに一致しているため、ポスチャ確認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確認に成功した後、EAPoUDP との通信が途絶えたピアの数。NAC Hold Timer アトリビュート（コンフィギュレーション > VPN > NAC）は、このタイプのイベントと、ピアごとの次のポスチャ確認試行間の遅延を指定します。
N/A	VPN NAC グループ ポリシーに応じて NAC がディセーブルになるピアの数。

表 30-8　show vpn-sessiondb summary コマンド：アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールド（続き）

フィールド	説明
Non-responsive	ポスチャ確認の際の EAP 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、これらの要求に応答しません。セキュリティ アプライアンス 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、アクセス コントロール サーバ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	ポスチャ確認に失敗したか、アクセス コントロール サーバによりアクセス ポリシーを供与されなかったピアの数。

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; Web キャッシュ通信プロトコル）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*]

シンタックスの説明

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	（オプション）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。番号は 0 ～ 256 の範囲です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスは値 99 で示されます。
detail	（オプション）ルータとすべての Web キャッシュに関する情報を表示します。
view	（オプション）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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

次の例では、WCCP 情報を表示する方法を示します。

```
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
asa1(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 がイネーブルになっているかどうかを判別し、イネーブルであった場合に、実行コンフィギュレーションの CSD バージョンを表示するか、または CSD の配布パッケージが有効かどうかを確認するためにファイルをテストするには、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*]

シンタックスの説明

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名を指定します。これは securedesktop_asa_<*n*>_<*n*>*.pkg の形式にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	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 モードに入って **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 はイネーブルです。フラッシュ デバイスから読み込まれた配布パッケージがバージョン番号を判別します。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る場合だけです。

ファイルが有効な CSD 配布パッケージであるかどうかをテストして確認するには、**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** コマンドが入力された場合は、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限り、CSD がインストールされます。ファイルが無効である場合は、「ERROR: Unable to use CSD image」のメッセージが表示されます。

show webvpn csd image コマンドは、有効な CSD 配布パッケージであるかどうかを確認するためにファイルをテストしますが、ファイルが有効な場合でも、自動的に CSD が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。形式が正しい場合は、ファイルを次の Web サイトから新たに取得したファイルで置き換えます。

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

次に **show webvpn csd image** コマンドを再入力します。イメージが有効である場合は、webvpn コンフィギュレーション モードで **csd image** および **csd enable** コマンドを使用して、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、CLI の応答にはバージョンと日付スタンプが含まれることに注意してください。

例

次の例は、CSD が実行コンフィギュレーションにインストールされてイネーブルにされたことを示しています。

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

次の例は、指定されたファイルが有効な CSD イメージであることを示しています。

```
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	コマンドで指定された CSD イメージを、パスで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*]

シンタックスの説明

tunnel-group	（オプション）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 グループ名を入力しない場合、このコマンドはすべてのトンネル グループのすべてのエイリアスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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ときには、WebVPN が実行されている必要があります。

各トンネル グループは、エイリアスを複数持つことも、まったく持たないこともあります。

例

次の例は、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、そのコマンドの出力を示しています。

```
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 つまたは複数の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

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*]

シンタックスの説明

tunnel-group	（オプション）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 グループ名を入力しない場合、このコマンドはすべてのトンネル グループのすべての URL を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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ときには、WebVPN が実行されている必要があります。各グループは、エイリアスを複数持つことも、まったく持たないこともあります。

例

次の例は、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、そのコマンドの出力を示しています。

```
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 つまたは複数の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

show webvpn sso-server

シングル サインオン サーバに関する動作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。これは CA SiteMinder コマンドによる SSO です。

show webvpn sso-server *name*

シンタックスの説明

name	SSO サーバの名前を指定します。文字数は最小 4 文字から最大 32 文字までです。

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

次の表は、このコマンドを入力できるモードを示しています。

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

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 1 度入力すると、再入力しなくてもさまざまなサーバで各種の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、設定済みである任意の SSO サーバまたはすべての SSO サーバの動作統計情報を表示します。

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

例

特権 EXEC モードで入力した次の例では、example という名前の SSO サーバの統計情報が表示されます。

```
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(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行が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 SSO 認証を要求する SSO サーバの URL を指定します。

show webvpn svc

SVC インストレーションを表示するか、有効な SVC ファイルかどうかを確認するためにファイルをテストするには、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*]

シンタックスの説明

image *filename*	SVC イメージ ファイルとしての有効性をテストするファイル名を指定します。

デフォルト

このコマンドには、デフォルトの動作も値もありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

使用するために設定された既存の SVC 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。

ファイルが有効な SVC イメージかどうかをテストして確認するには、**image** *filename* オプションを使用します。ファイルが有効な SVC イメージでない場合は、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

次の例は、現在インストールされている SVC イメージに対する **show webvpn svc** コマンドの出力を示しています。

```
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 15
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

次の例は、有効な SVC イメージに対する **show webvpn svc image** *filename* コマンドの出力を示しています。

```
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	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。