show running-config コマンド～ show switch vlan コマンド

show running-config

ASA 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するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**all**] [*command*]

構文の説明

all	デフォルトを含め、動作設定全体を表示します。
command	特定のコマンドに関連付けられたコンフィギュレーションを表示します。使用可能なコマンドについては、**show running-config ?** を使用して CLI ヘルプを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	暗号化されたパスワードが出力に追加されました。
9.7(1)	このコマンドの出力も、IPv6 アドレスで設定された syslog サーバを表示します。

使用上のガイドライン

show running-config コマンドは、ASA のメモリにあるアクティブなコンフィギュレーション（保存されたコンフィギュレーションの変更を含む）を表示します。

ASA のフラッシュ メモリに保存されたコンフィギュレーションを表示するには、**show configuration** コマンドを使用します。

show running-config コマンドの出力では、パスワードの暗号化がイネーブルかディセーブルかに応じて、パスワードが暗号化、マスク、またはクリア テキストの状態で表示されます。

（注） このコマンドを使用して ASA への接続または設定を行った後は、コンフィギュレーションに ASDM コマンドが表示されます。

ASA リリース 9.3 でディセーブルに変更された **error-recovery disable** のデフォルトです。そのため、WebVPN error recovery がデフォルト値の場合、**show running-config** コマンドは *error-recovery disable* を CLI に 表示するようになりました。問題のトラブルシューティング時にシスコのテクニカル アシスタンス センターからの指示がない限り、これはディセーブルのままにしておくことを推奨します。

例

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

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
```

```
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
```

```
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

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

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

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

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
show configuration	スタートアップ コンフィギュレーションを表示します。

show saml metadata

SAML メタデータのトンネル グループ名を表示します。

show saml metadata tunnel-group-name

構文の説明

SAML メタデータを表示するトンネル グループの名前を入力します。

コマンド デフォルト

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	• Yes

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

特定のトンネル グループの SAML SP のメタデータを表示します。

例

show scansafe server コマンドのサンプル出力を次に示します。

```
ciscoasa# show saml metadata saml_sso_tunnel_group
```

関連コマンド

コマンド	説明
saml idp	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。

show scansafe server

クラウド Web セキュリティ プロキシ サーバのステータスを表示するには、特権 EXEC モードで **show scansafe server** コマンドを使用します。

show scansafe server

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。

コマンド デフォルト

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	• Yes

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。

マルチ コンテキスト モードでは、このコマンドの出力は、ScanSafe サーバに到達する管理コンテキストの機能によって異なります。管理コンテキストは、定期的にポーリングを試行して、トラフィックが ASA を通過していない場合に ScanSafe サーバがアップしているかどうかを確認します。ポーリング試行の間隔は設定不可で、15 分に固定されています。また、管理コンテキストは、ScanSafe タワーにキープアライブを送信します。

例

show scansafe server コマンドのサンプル出力を次に示します。

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
ホワイトリスト	トラフィックのクラスでホワイトリスト アクションを実行します。

show scansafe statistics

クラウド Web セキュリティ アクティビティに関する情報を表示するには、特権 EXEC モードで **show scansafe statistics** コマンドを使用します。

show scansafe 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。

コマンド デフォルト

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	—	• Yes

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show scansafe statistics コマンドは、プロキシ サーバにリダイレクトされる接続数、現在リダイレクトされている接続数、ホワイトリストに記載されている接続数などのクラウド Web セキュリティ アクティビティに関する情報を示します。

例

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

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
ホワイトリスト	トラフィックのクラスでホワイトリスト アクションを実行します。

show sctp

現在の Stream Control Transmission Protocol（SCTP）Cookie とアソシエーションを表示するには、特権 EXEC モードで **show sctp** コマンドを使用します。

show sctp [**detail**]

構文の説明

detail	SCTP アソシエーションに関する詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。
9.7(1)	詳細な出力に、マルチホーミング、複数のストリーム、およびフレームリアセンブルに関する情報が含まれるようになりました。

使用上のガイドライン

show sctp コマンドは、SCTP Cookie とアソシエーションに関する情報を表示します。

例

次に、**show sctp** コマンドの出力例を示します。

```
ciscoasa# show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

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

```
ciscoasa(config)# show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

9.7(1) から、詳細な出力に、マルチホーミング、複数のストリームおよびフレーム リアセンブルに関する情報が含まれるようになりました。

```
asa2005# show sctp detail

AssocID: 2e590263
Local:  10.0.103.250/50000 (ESTABLISHED)
    Multi-homing IP's: 10.0.103.251(10.0.103.251)
    Receiver Window: 106496
    Cumulative TSN: bf0a3180
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
    Stream ID 3: next SN 10, first/last queued SN 11/16, hole SN:
    Stream ID 4: next SN 10, first/last queued SN 11/16, hole SN:
Remote: 10.0.102.250/3868 (CLOSED)
    Multi-homing IP's: 10.0.102.251(10.0.102.251)
    Receiver Window: 106496
    Cumulative TSN: 915d5916
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
Secondary Conn List:
    10.0.102.251(10.0.102.251):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.251(10.0.102.251):3868
    10.0.102.250(10.0.102.250):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.250(10.0.102.250):3868
    10.0.102.251(10.0.102.251):3868 to 10.0.103.250(10.0.103.250):50000
    10.0.103.250(10.0.103.250):50000 to 10.0.102.251(10.0.102.251):3868
```

関連コマンド

コマンド	説明
show local-host	インターフェイスごとに、ASA 経由で接続を確立しているホストの情報を表示します。
show service-policy inspect sctp	SCTP インスペクションの統計情報を表示します。
show traffic	インターフェイスごとに、接続とインスペクションの統計情報を表示します。

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** | **cxsc** | **inspect** *inspection* [*arguments*] | **ips** | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]

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	（オプション）**csc** コマンドを含むポリシーに関する詳細情報を表示します。
cxsc	（オプション）**cxsc** コマンドを含むポリシーに関する詳細情報を表示します。
dest_ip dest_mask	**flow** キーワードに対する宛先 IP アドレスおよびトラフィック フローのネットマスク。
details	（オプション）**set connection** キーワードの場合、クライアントごとの接続制限がイネーブルな場合に、クライアントごとの接続情報を表示します。
eq *dest_port*	**flow** キーワードの場合、この値に等しいフローの宛先ポートに相当します。
eq *src_port*	（オプション）**flow** キーワードの場合、この値に等しいフローの送信元ポートに相当します。
flow *protocol*	（オプション）5 つのタプル（プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート）で識別される特定フローに一致するポリシーを示します。このコマンドを利用すると、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。 フローが 5 つのタプルとして示されるため、すべてのポリシーがサポートされるわけではません。次のサポート対象ポリシーが一致します。 • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	（オプション）出力をグローバル ポリシーに制限します。
host *dest_host*	**flow** キーワードに対するトラフィック フローのホスト宛先 IP アドレス。
host *src_host*	**flow** キーワードに対するトラフィック フローのホスト送信元 IP アドレス。
icmp_control_message	（オプション）プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、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_number	(オプション)プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、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 *inspection* [*arguments*]	(オプション)**inspect** コマンドを含むポリシーに関する詳細情報を表示します。詳細出力では、一部の **inspect** コマンドはサポートされません。すべてのインスペクションを表示するには、引数を使用せずに **show service-policy** コマンドを使用します。各インスペクションで使用できる引数は異なります。詳細については、CLI ヘルプを参照してください。
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	(オプション)**ips** コマンドを含むポリシーに関する詳細情報を表示します。
police	(オプション)**police** コマンドを含むポリシーに関する詳細情報を表示します。
priority	(オプション)**priority** コマンドを含むポリシーに関する詳細情報を表示します。
set connection	(オプション)**set connection** コマンドを含むポリシーに関する詳細情報を表示します。
sfr	(オプション)**sfr** コマンドを含むポリシーに関する詳細情報を表示します。
shape	(オプション)**shape** コマンドを含むポリシーに関する詳細情報を表示します。
src_ip src_mask	**flow** キーワードに対する送信元 IP アドレスおよびトラフィック フローで使用されるネットマスク。
user-statistics	(オプション)**user-statistics** コマンドを含むポリシーに関する詳細情報を表示します。このコマンドは、アイデンティティ ファイアウォールに関するユーザ統計情報を表示します。これには、選択したユーザの、送信パケット数、送信ドロップ数、受信パケット数および送信ドロップ数が含まれます。

デフォルト

引数を指定しない場合、このコマンドはすべてのグローバル ポリシーおよびインターフェイス ポリシーを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
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。
8.4(2)	アイデンティティ ファイアウォール用の **user-statistics** キーワードのサポートが追加されました。
8.4(4.1)	ASA CX モジュール用の **cxsc** キーワードのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュール用の **sfr** キーワードのサポートが追加されました。
9.5(2)	**inspect sctp** および **inspect diameter** キーワードが追加されました。
9.6(2)	**inspect stun** および **inspect m3ua** {**drops** | **endpoint** *ip_address*} キーワードが追加されました。
9.7(1)	**inspect m3ua session** キーワードと **inspect gtp pdpmcb teid** *teid* キーワードが追加されました。また、表示ルールの制限がクラス マップあたり 64 から 128 に引き上げられました。

使用上のガイドライン

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、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。

コンフィギュレーションに対してサービス ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいサービス ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータが含まれていません。たとえば、インターフェイスから QoS サービス ポリシーを削除し、変更したバージョンを再度追加した場合、**show service-policy** コマンドには、新しいサービス ポリシーに一致する新しい接続に関連付けられた QoS カウンタだけが表示されます。古いポリシーの既存の接続はコマンド出力には表示されなくなります。すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** または **clear local-host** コマンドを参照してください。

（注） **inspect icmp** および **inspect icmp error** ポリシーの場合、パケット数にはエコー要求パケットと応答パケットのみが含まれます。

例

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

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# 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。

```
ciscoasa# 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
```

複数の CPU コアを搭載しているデバイスの場合は、ロック失敗用のカウンタがあります。共有されるデータ構造と変数は複数のコアによって使用可能なため、それらを保護するためにロック メカニズムが使用されます。コアはロックの取得に失敗すると、ロックの取得を再試行します。ロック失敗カウンタは、試行が失敗するごとに増分されます。

```
ciscoasa# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

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。

```
ciscoasa# 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
```

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。出力については、表 12-1 で説明されています。

```
firewall(config)# 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                   67     total_dropped              1
  signalling_msg_dropped             1     data_msg_dropped           0
  signalling_msg_forwarded          67     data_msg_forwarded         0
  total created_pdp                 33     total deleted_pdp          32
  total created_pdpmcb              31     total deleted_pdpmcb       30
  total dup_sig_mcbinfo              0     total dup_data_mcbinfo     0
  no_new_sgw_sig_mcbinfo             0     no_new_sgw_data_mcbinfo    0
  pdp_non_existent                   1
```

表 12-1　GPRS GTP 統計情報

カラムのヘッダー	説明
version_not_support	サポートされていない GTP バージョン フィールドを持つパケットの数を表示します。
msg_too_short	長さが 8 バイトより短いパケットの数を表示します。
unknown_msg	不明なタイプのメッセージ数を表示します。
unexpected_sig_msg	予期しないシグナリング メッセージ数を表示します。
unexpected_data_msg	予期しないデータ メッセージ数を表示します。

表 12-1　GPRS GTP 統計情報（続き）

カラムのヘッダー	説明
mandatory_ie_missing	必須情報要素（IE）が欠落しているメッセージ数を表示します。
mandatory_ie_incorrect	不正な形式の必須情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	無効なオプション情報要素（IE）を持つメッセージ数を表示します。
ie_unknown	不明な情報要素（IE）を持つメッセージ数を表示します。
ie_out_of_order	順番どおりでない情報要素（IE）を持つメッセージ数を表示します。
ie_unexpected	予期しない情報要素（IE）を持つメッセージを表示します。
ie_duplicated	重複した情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	不正な形式のオプション情報要素（IE）を持つメッセージ数を表示します。
total_dropped	ドロップされたメッセージの合計数を表示します。
signalling_msg_dropped	ドロップされた信号メッセージ数を表示します。
data_msg_dropped	ドロップされたデータ メッセージ数を表示します。
total_forwarded	転送されたメッセージの合計数を表示します。
signalling_msg_forwarded	転送された信号メッセージ数を表示します。
data_msg_forwarded	転送されたデータ メッセージ数を表示します。
total created_pdp	作成されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。
total deleted_pdp	削除されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	これらのフィールドは、実装機能である PDP マスター制御ブロックの使用に関連しています。これらのカウンタは、トラブルシューティング向けにシスコ テクニカル サポートによって使用され、エンドユーザには直接の関係はありません。
pdp_non_existent	存在しない PDP コンテキストに対して受信したメッセージ数を表示します。

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。

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 32 most used

Version TID                  MS Addr         SGSN Addr    Idle      Timeout   APN
v2      2692026893437055 10.0.0.1        10.0.0.11       0:00:11  0:04:00
gprs.example.com
```

ASA 9.6.2 以降、GTP PDP コンテキスト情報はテーブルではなく、1 行ずつ示されます。このため、IPv6 アドレスの使用時に、情報が読み取り易くなります。

```
ciscoasa# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 0505420121517705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

表 12-2 に、**show service-policy inspect gtp pdp-context** コマンドの出力の説明を示します。

表 12-2　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 SGW Addr	サービング ゲートウェイ サービス ノード（SGSN）またはサービング ゲートウェイ（SGW）を表示します。
Idle	PDP またはベアラー 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
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 shared license

共有ライセンス統計情報を表示するには、特権 EXEC モードで **show shared license** コマンドを使用します。オプションのキーワードはライセンス サーバのみで使用できます。

show shared license [**detail** | **client** [*hostname*] | **backup**]

構文の説明

バックアップ	(任意)バックアップ サーバに関する情報を表示します。
クライアント	(任意)参加ユニットの情報だけを表示します。
detail	(任意)参加ユニットごとの統計情報を含む、すべての統計情報を表示します。
hostname	(任意)特定の参加ユニットの情報だけを表示します。

コマンド デフォルト

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

統計情報をクリアするには、**clear shared license** コマンドを入力します。

例

次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
```

```
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

表 12-3 に、**show shared license** コマンドの出力を示します。

表 12-3　show shared license の説明

フィールド	説明
Primary License Server	プライマリ サーバの IP アドレス。
Version	共有ライセンスのバージョン。
Status（ステータス）	コマンドがバックアップ サーバで発行された場合、「Active」はこのデバイスがプライマリ共有ライセンス サーバとしての役割を果たしていることを意味します。「Inactive」は、デバイスがスタンバイ モードで待機しており、デバイスはプライマリ サーバと通信していることを意味します。 フェールオーバー ライセンスがプライマリ サーバで設定されると、バックアップ サーバは、フェールオーバー中、瞬間的に「Active」になりますが、通信の同期が再び完了すると「Inactive」に戻ります。
Shared license utilization	
SSLVPN	
Total for network	使用可能な共有セッションの合計数が表示されます。
Available	使用できる残りの共有セッションを表示します。
Utilized	アクティブなライセンス サーバに対して取得された共有セッション数を表示します。
This device	
Platform limit	インストールされているライセンス応じて、デバイスの SSL VPN セッションの合計数を表示します。
現在の使用状況	現在このデバイスが所有する、共有プールからの共有 SSL VPN セッション数を表示します。
High usage	このデバイスが所有した共有 SSL VPN セッションの最大数を表示します。
Messages Tx/Rx/Error	
登録 get リリース Transfer	各接続タイプの送信、受信およびエラーのパケット数を示します。
Client ID	一意のクライアント ID。

表 12-3　show shared license の説明（続き）

フィールド	説明
使用法	使用中のセッション数を表示します。
Hostname	このデバイスのホスト名を表示します。

次に、ライセンス サーバ上での **show shared license detail** コマンドの出力例を示します。

```
ciscoasa# show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。

コマンド	説明
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

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。
統計情報	(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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

例

次に、**show shun** コマンドの出力例を示します。

```
ciscoasa# 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show sip コマンドは、ASA 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。

（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。

```
ciscoasa# 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、ASA 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
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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）セッションに関する情報を表示します。

例

次の条件での **show skinny** コマンドの出力例を示します。ASA 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。

```
ciscoasa# show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
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。

関連コマンド

コマンド	説明
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	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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。

```
ciscoasa> 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:

ciscoasa# 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	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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。

```
ciscoasa> 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 engineid

ASA 上で設定されている SNMP エンジンの ID を表示するには、特権 EXEC モードで **show snmp-server engineid** コマンドを使用します。

show snmp-server engineid

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

使用上のガイドライン

SNMP エンジンは、ローカル デバイス上に配置できる SNMP のコピーです。エンジン ID は、各 ASA コンテキストの SNMP エージェントごとに割り当てられる固有の値です。ASA ではエンジン ID を設定できません。エンジン ID の長さは 25 バイトで、この ID は暗号化されたパスワードの生成に使用されます。暗号化されたパスワードはフラッシュ メモリに保存されます。エンジン ID はキャッシュすることができます。フェールオーバー ペアでは、エンジン ID がピアと同期化されます。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
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。
snmp-server	SNMP サーバを設定します。

show snmp-server group

設定済みの SNMP グループの名前、使用するセキュリティ モデル、さまざまなビューのステータス、および各グループのストレージ タイプを表示するには、特権 EXEC モードで **show snmp-server group** コマンドを使用します。

show snmp-server group

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                    security model:v3 priv
readview : def_read_view                writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

使用上のガイドライン

SNMP ユーザおよび SNMP グループは、SNMP の View-based Access Control Model（VACM）に従って使用されます。使用されるセキュリティ モデルは、SNMP グループによって決まります。SNMP ユーザは、SNMP グループのセキュリティ モデルに一致する必要があります。各 SNMP グループ名とセキュリティ レベルのペアは一意である必要があります。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
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。
snmp-server	SNMP サーバを設定します。

show snmp-server host

ホスト グループに属する設定済みの SNMP ホストの名前、使用されているインターフェイスおよび使用されている SNMP のバージョンを表示するには、特権 EXEC モードで **show snmp-server host** コマンドを使用します。

show snmp-server host

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.4(1)	出力は、ASA をポーリングしているアクティブなホストと、静的に設定されているホストのみを表示するように更新されました。

例

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

```
ciscoasa# show snmp-server host
host ip = 10.10.10.1, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.10, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.2, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.4, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.5, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.7, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.8, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.9, interface = mgmt  poll community ***** version 2c
```

次に、Version 9.4(1) 現在の **show snmp-server host** コマンドの出力例を示します。ASA をポーリングしているアクティブなホストのみが表示されます。

```
ciscoasa# show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
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。
snmp-server	SNMP サーバを設定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# 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
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
clear snmp-server statistics	SNMP パケットの入力カウンタおよび出力カウンタをクリアします。
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。
snmp-server	SNMP サーバを設定します。

show snmp-server user

設定されている SNMP ユーザの特性に関する情報を表示するには、特権 EXEC モードで **show snmp-server user** コマンドを使用します。

show snmp-server user [*username*]

構文の説明

username	（任意）SNMP 情報を表示する特定のユーザ（複数可）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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

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

```
ciscoasa# show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

この出力には次の情報が表示されます。

- ユーザ名。SNMP ユーザの名前を識別するストリングです。
- エンジン ID。ASA 上の SNMP のコピーを識別するストリングです。
- ストレージ タイプ。ASA の揮発性メモリまたは一時メモリに設定が格納されているか、あるいは不揮発性メモリまたは永続メモリに格納されているかを示します。非揮発性メモリまたは永続メモリに格納されている場合、ASA をオフにして再度オンにした場合でも設定は存続します。
- アクティブなアクセス リスト。SNMP ユーザに関連付けられている標準の IP アクセス リストです。

- Rowstatus。ユーザがアクティブか非アクティブかを示します。
- 認証プロトコル。使用されている認証プロトコルを示します。選択できるのは、MD5、SHA、なしのいずれかです。ソフトウェア イメージで認証がサポートされていない場合、このフィールドは表示されません。
- プライバシー プロトコル。DES によるパケット暗号化がイネーブルかどうかを示します。ソフトウェア イメージでプライバシーがサポートされていない場合、このフィールドは表示されません。
- グループ名。ユーザが属している SNMP グループを示します。SNMP グループは、View-based Access Control Model（VACM）に従って定義されます。

使用上のガイドライン

SNMP ユーザは、SNMP グループの一部である必要があります。*username* 引数が入力されなかった場合、**show snmp-server user** コマンドには設定済みのすべてのユーザに関する情報が表示されます。*username* 引数が入力され、そのユーザが存在する場合は、指定したユーザに関する情報が表示されます。

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
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。
snmp-server	SNMP サーバを設定します。

show software authenticity development

開発キー署名イメージのロードが有効または無効になっていることを確認するには、特権 EXEC モードで **show software authenticity development** コマンドを使用します。

show software authenticity development

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity file** コマンドの出力例を示します。

```
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

関連コマンド

コマンド	説明
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します。
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。

コマンド	説明
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。
show software authenticity	特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示します。

show software authenticity file

特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示するには、特権 EXEC モードで **show software authenticity file** コマンドを使用します。

show software authenticity [*filename*]

構文の説明

filename	(オプション)特定のイメージ ファイルを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity file** コマンドの出力例を示します。

```
ciscoasa# show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

この出力には次の情報が表示されます。

- メモリ内のファイルの名前であるファイル名。
- 表示されるイメージのタイプであるイメージ タイプ。
- 署名者情報によって、次のようなシグニチャ情報が指定されます。
  - 一般名。ソフトウェア メーカーの名前です。
  - 組織単位。ソフトウェア イメージが展開されるハードウェアを示します。
  - 組織名。ソフトウェア イメージの所有者です。

- 証明書シリアル番号。デジタル署名の証明書シリアル番号です。
- ハッシュ アルゴリズム。デジタル署名確認に使用されるハッシュ アルゴリズムのタイプを示します。
- 署名アルゴリズム。デジタル署名確認に使用される署名アルゴリズムのタイプを識別します。
- キー バージョン。確認に使用されるキー バージョンを示します。

関連コマンド

コマンド	説明
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します。

show software authenticity keys

SPI フラッシュに格納されている開発キーおよびリリース キーの情報を表示するには、特権 EXEC モードで **show software authenticity keys** コマンドを使用します。

show software authenticity keys

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。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity keys** コマンドの出力例を示します。

```
ciscoasa# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
```

```
Exponent              : 65537
Key Version           : A
Public Key #2 Information
--------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #3 Information
--------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

関連コマンド

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity keys	開発キーを表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

コマンド	説明
software authenticity key add special	SPR フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPR フラッシュから古い開発キーを削除します。

show software authenticity running

特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示するには、特権 EXEC モードで **show software authenticity running** コマンドを使用します。このコマンドは、現在実行中のファイルに関連したデジタル署名情報を表示することを除き、**show software authenticity file** と同じです。

show software authenticity running

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

例

次に、**show software authenticity running** コマンドの出力例を示します。

```
ciscoasa# show software authenticity running
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 5448091A
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : Cisco Systems ROMMON,1.0.16
```

この出力には次の情報が表示されます。

- メモリ内のファイルの名前であるファイル名。
- 表示されるイメージのタイプであるイメージ タイプ。

- 署名者情報によって、次のようなシグニチャ情報が指定されます。
  - 一般名。ソフトウェア メーカーの名前です。
  - 組織単位。ソフトウェア イメージが展開されるハードウェアを示します。
  - 組織名。ソフトウェア イメージの所有者です。
- 証明書シリアル番号。デジタル署名の証明書シリアル番号です。
- ハッシュ アルゴリズム。デジタル署名確認に使用されるハッシュ アルゴリズムのタイプを示します。
- 署名アルゴリズム。デジタル署名確認に使用される署名アルゴリズムのタイプを識別します。
- キー バージョン。確認に使用されるキー バージョンを示します。

関連コマンド

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
software authenticity key add special	SPR フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPR フラッシュから古い開発キーを削除します。

show ssh sessions

ASA 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 [**hostname** or **A.B.C.D**] [**hostname** or **X:X:X:X::X**] [**detail**]

構文の説明

hostname or **A.B.C.D**	（オプション）指定された SSH クライアント IPv4 アドレスのみの SSH セッション情報を表示します。
hostname or **X:X:X:X::X**	（オプション）指定された SSH クライアント IPv6 アドレスのみの SSH セッション情報を表示します。
detail	SSH セッションの詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(2)	**detail** オプションが追加されました。

使用上のガイドライン

SID は、SSH セッションを識別する一意の番号です。Client IP は、SSH クライアント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 ASA 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。

```
ciscoasa# 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
```

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

```
ciscoasa# show ssh sessions detail
SSH Session ID              : 0
>   Client IP               : 161.44.66.200
>   Username                : root
>   SSH Version             : 2.0
>   State                   : SessionStarted
>   Inbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Received         : 2224
>   Outbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Transmitted      : 2856
>   Rekey Information
>    Time Remaining (sec)   : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey             : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys      : 0
>    Time-Based Rekeys      : 0
```

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 ssl

ASA 上の SSL 設定およびアクティブな SSL 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 ssl** コマンドを使用します。

show ssl [**cache** | **ciphers** [*level*] | **errors** | **mib** | **objects**]

構文の説明

cache	（オプション）SSL セッション キャッシュの統計情報を表示します。
ciphers [*level*]	（オプション）**ssl cipher** コマンドを使用して設定したレベルに基づき、使用するために設定されている暗号方式を表示します。次のいずれかのレベルを指定すると、そのレベルの暗号方式のみを表示できます。レベルを指定しない場合、中間レベルの SSL、TLS、DTLS の各バージョンが表示されます。 • **all**：すべての暗号方式が含まれます。 • **low**：NULL-SHA を除くすべての暗号が含まれます。 • **medium**：NULL、DES、RC4 の暗号方式を除くすべての暗号方式が含まれます。 • **fips**：すべての FIPS 準拠の暗号方式が含まれます。 • **high**：TLSv1.2 にのみ適用され、最も強力な暗号方式のみが含まれます。
errors	（オプション）SSL エラーを表示します。
mib	（オプション）SSL MIB の統計情報を表示します。
オブジェクト	（オプション）SSL オブジェクト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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	**detail** オプションが追加されました。
9.3(2)	TLSv1.1 および TLSv1.2 のサポートが追加されました。**ciphers** キーワードが追加されました。

使用上のガイドライン

このコマンドは、現在の SSLv2 および SSLv3 セッションに関する情報を表示します。情報には、イネーブルにされた暗号の順序、ディセーブルにされた暗号、使用されている SSL トラストポイント、証明書認証がイネーブルかどうか、などが含まれます。

例

次に、**show ssl** コマンドの出力例を示します。

```
ciscoasa# show ssl

Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2

SSL trust-points:
  Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

次に、**show ssl ciphers fips** コマンドの出力例を示します。

```
ciscoasa# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

次に、**show ssl ciphers** コマンドの出力を示します。

```
ciscoasa# show ssl ciphers all
These are the ciphers for the given cipher level; not all ciphers
are supported by all versions of SSL/TLS.
These names can be used to create a custom cipher list
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
```

```
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (tlsv1)
  RC4-MD5 (tlsv1)
  DES-CBC-SHA (tlsv1)
  NULL-SHA (tlsv1)
asa3(config-tlsp)# show ssl ciphers medium
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
```

```
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
```

関連コマンド

コマンド	説明
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
ssl ciphers	SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。

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）ASA 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	トランスペアレント	シングル	コンテキスト	システム[1]
特権 EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

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。
8.3(1)	暗号化されたパスワードが出力に追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、**show startup-config** 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。

show startup-config コマンドの出力では、パスワードの暗号化が有効か無効かに応じて、パスワードが暗号化、マスク、またはクリア テキストの状態で表示されます。

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。

```
ciscoasa# 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 209.165.200.224
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 209.165.200.225
!

...
!
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 209.165.200.226
!
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。

```
ciscoasa# 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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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。

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

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバの IP アドレスを示します。

関連コマンド

コマンド	説明
clear configure sunrpc-server	ASA 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。

コマンド	説明
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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、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。

```
ciscoasa# 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 12-4 に、各フィールドの説明を示します。

表 12-4　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。
タイプ	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、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。

```
ciscoasa# 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 12-5 に、各フィールドの説明を示します。

表 12-5　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。
名前	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(ステータス)	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。
ポート	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。