CHAPTER 26

show ddns update interface コマンド～ show ipv6 traffic コマンド

show ddns update interface

セキュリティ アプライアンス インターフェイスに割り当てられた DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを使用します。

show ddns update interface [*interface-name*]

構文の説明

interface-name	（任意）ネットワーク インターフェイスの名前。

デフォルト

interface-name ストリングを省略すると、各インターフェイスに割り当てられている DDNS 方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、内部インターフェイスに割り当てられている DDNS 方式を表示する例を示します。

```
hostname# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
hostname#
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update method	設定済みの DDNS 方式ごとにタイプと間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show ddns update method

実行コンフィギュレーションの DDNS 更新方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

show ddns update method [*method-name***]**

構文の説明

method-name	（任意）設定済み DDNS 更新方式の名前。

デフォルト

method-name ストリングを省略すると、設定されているすべての DDNS 更新方式が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、ddns-2 という名前の DDNS 方式を表示する例を示します。

```
hostname(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
hostname(config)#
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを Dynamic DNS（DDNS; ダイナミック DNS）更新方式または DDNS 更新ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられたインターフェイスを表示します。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

show debug

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

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

構文の説明

command	（任意）現在のコンフィギュレーションを表示する対象のデバッグ コマンドを指定します。各 *command* では、*command* の後の構文は、関連する **debug** コマンドでサポートされる構文と同一です。たとえば、**show debug aaa** の後に続く有効な *keywords* は、**debug aaa** コマンドの有効なキーワードと同じです。したがって、**show debug aaa** は **accounting** キーワードをサポートし、このキーワードによって AAA デバッグのその部分についてのデバッグ コンフィギュレーションを表示することを指定できます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
8.0(2)	使用可能なコマンド値のリストに **eigrp** キーワードが追加されました。

使用上のガイドライン

有効な *command* 値が後に続きます。各 *command* では、*command* の後の構文は、関連する **debug** コマンドでサポートされる構文と同一です。サポートされている構文については、関連する **debug** コマンドを参照してください。

（注）　各 *command* 値を使用できるかどうかは、該当する **debug** コマンドをサポートするコマンド モードによって決まります。

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**

- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

例

次のコマンドでは、認証、アカウンティング、およびフラッシュ メモリのデバッグをイネーブルにします。**show debug** コマンドが 3 通りの方法で使用され、すべてのデバッグ コンフィギュレーション、特定機能のデバッグ コンフィギュレーション、機能のサブセットのデバッグ コンフィギュレーションを表示するためのコマンドの使用方法が示されています。

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
```

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

関連コマンド

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

show debug mmp

MMP インスペクション モジュールの現在のデバッグ設定を表示するには、特権 EXEC モードで **show debug mmp** コマンドを使用します。

show debug mmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、MMP インスペクション モジュールの現在のデバッグ設定を表示するために **show debug mmp** コマンドを使用する例を示します。

```
hostname# show debug mmp
debug mmp  enabled at level 1
```

関連コマンド

コマンド	説明
debug mmp	MMP イベントのインスペクションを表示します。
inspect mmp	MMP インスペクション エンジンを設定します。

show dhcpd

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

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

構文の説明

binding	所定のサーバ IP アドレスおよび関連するクライアント ハードウェア アドレスについてのバインディング情報とリースの長さを表示します。
IP_address	指定した IP アドレスのバインディング情報を表示します。
state	DHCP サーバの状態（現在のコンテキストでイネーブルかどうか、各インターフェイスについてイネーブルかどうかなど）を表示します。
statistics	統計情報（アドレス プール、バインディング、期限切れバインディング、不正な形式のメッセージ、送信済みメッセージ、および受信メッセージなどの数）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

オプションの IP アドレスを **show dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけが表示されます。

show dhcpd binding | state | statistics コマンドはグローバル コンフィギュレーション モードでも使用可能です。

例

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

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

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

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

```
Interface inside, Not Configured for DHCP
```

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

```
hostname# show dhcpd statistics

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

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

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

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

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
clear dhcpd	DHCP サーバ バインディングおよび統計情報カウンタをクリアします。
dhcpd lease	クライアントに付与される DHCP 情報のリースの長さを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

show dhcprelay state

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

show dhcprelay state

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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

例

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

```
hostname# show dhcprelay state

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

関連コマンド

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

show dhcprelay statistics

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

show dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show dhcprelay statistics コマンドの出力は、**clear dhcprelay statistics** コマンドを入力するまで増加します。

例

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

```
hostname# show dhcprelay statistics

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

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

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
hostname#
```

関連コマンド

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

show disk

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

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

構文の説明

0	**1**	内部フラッシュ メモリ（0、デフォルト）または外部フラッシュ メモリ（1）を指定します。
controller	フラッシュ コントローラのモデル番号を指定します。
filesys	コンパクト フラッシュ カードの情報を表示します。
all	フラッシュ メモリの内容およびファイル システム情報を表示します。

デフォルト

デフォルトでは内部フラッシュ メモリを表示します。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show disk** コマンドの出力例を示します。

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

```
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

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

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

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

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

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

```
hostname# show disk1: controller
Flash Model: TOSHIBA THNCF064MBA
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show flash	PIX セキュリティ アプライアンス専用の内部フラッシュ メモリの内容を表示します。

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバからダイナミックに学習したエントリと、**name** コマンドを使用して手動で入力された名前および IP アドレスが含まれています。

show dns-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show dns-hosts** コマンドの出力例を示します。

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

表 11 に、各フィールドの説明を示します。

表 26-1　show dns-hosts の各フィールド

フィールド	説明
Host	ホスト名を表示します。
Flags	次の組み合わせとしてエントリのステータスを表示します。 • temp：このエントリは DNS サーバから取得されたため、一時的です。セキュリティ アプライアンスは、72 時間の無活動後にこのエントリを削除します。 • perm：このエントリは **name** コマンドを使用して追加されたため、永続的です。 • OK：このエントリは有効です。 • ??：このエントリは疑わしいため、再検証が必要です。 • EX：このエントリは期限切れです。
Age	このエントリが最後に参照されてからの時間数を表示します。
Type	DNS レコードのタイプを表示します。この値は常に IP です。
Address(es)	IP アドレス。

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュをクリアします。
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。

show eigrp events

EIGRP イベント ログを表示するには、特権 EXEC モードで **show eigrp events** コマンドを使用します。

show eigrp [*as-number*] **events** [{*start end*} | **type**]

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
end	（任意）出力されるエントリを、インデックス番号 *start* で開始され、インデックス番号 *end* で終了するエントリに限定します。
start	（任意）ログ エントリのインデックス番号を指定する数値。開始番号を指定すると、出力は指定されたイベントで開始し、*end* 引数で指定されたイベントで終了します。有効な値は、1 ～ 4294967295 です。
type	（任意）記録されるイベントを表示します。

デフォルト

start および *end* を指定しない場合、すべてのログ エントリが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show eigrp events の出力では最大 500 件のイベントが表示されます。イベントが最大数に到達すると、新しいイベントは出力の末尾に追加され、古いイベントは出力の先頭から削除されます。

clear eigrp events コマンドを使用すると、EIGRP イベント ログをクリアできます。

show eigrp events type コマンドは、EIGRP イベントのロギング ステータスを表示します。デフォルトでは、ネイバー変更、ネイバー警告、および DUAL FSM メッセージが記録されます。ネイバー変更イベントのロギングは、**no eigrp log-neighbor-changes** コマンドを使用してディセーブルにできます。ネイバー警告イベントのロギングは、**no eigrp log-neighbor-warnings** コマンドを使用してディセーブルにできます。DUAL FSM イベントのロギングはディセーブルにできません。

例

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

```
hostname# show eigrp events
```

```
Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

次に、**show eigrp events** コマンドで開始番号と終了番号を定義したときの出力例を示します。

```
hostname# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

次に、EIGRP イベント ログのエントリがない場合の **show eigrp events** コマンドの出力例を示します。

```
hostname# show eigrp events

Event information for AS 100:  Event log is empty.
```

次に、**show eigrp events type** コマンドの出力例を示します。

```
hostname# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

関連コマンド

コマンド	説明
clear eigrp events	EIGRP イベント ロギング バッファをクリアします。
eigrp log-neighbor-changes	ネイバー変更イベントのロギングをイネーブルにします。
eigrp log-neighbor-warnings	ネイバー警告イベントのロギングをイネーブルにします。

show eigrp interfaces

EIGRP ルーティングに参加しているインターフェイスを表示するには、特権 EXEC モードで **show eigrp interfaces** コマンドを使用します。

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

構文の説明

as-number	（任意）アクティブ インターフェイスを表示する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	（任意）詳細情報を表示します。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、指定されたインターフェイスに表示が制限されます。

デフォルト

インターフェイス名を指定しない場合、すべての EIGRP インターフェイスの情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show eigrp interfaces コマンドを使用して、EIGRP がアクティブなインターフェイスを判別し、それらのインターフェイスに関連する EIGRP についての情報を学習します。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティング プロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

例

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

```
hostname# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
```

```
mgmt          0          0/0           0       11/434           0           0
outside       1          0/0         337         0/10           0           0
inside        1          0/0          10         1/63         103           0
```

表 26-2 に、この出力で表示される重要なフィールドの説明を示します。

表 26-2　show eigrp interfaces のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Peers	直接接続されているピアの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均のスムーズ ラウンドトリップ時間間隔（秒）。
Pacing Time Un/Reliable	EIGRP パケット（信頼性の低いパケットおよび信頼性の高いパケット）をインターフェイスに送信するタイミングを決定するために使用されるペーシング時間（秒）。
Multicast Flow Timer	セキュリティ アプライアンスがマルチキャスト EIGRP パケットを送信する最大秒数。
Pending Routes	送信キュー内で送信を待機しているパケット内のルートの数。

関連コマンド

コマンド	説明
network	EIGRP ルーティング プロセスに参加するネットワークおよびインターフェイスを定義します。

show eigrp neighbors

EIGRP ネイバー テーブルを表示するには、特権 EXEC モードで **show eigrp neighbors** コマンドを使用します。

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
detail	（任意）詳細なネイバー情報を表示します。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定する場合、そのインターフェイスを介して学習されたすべてのネイバー テーブル エントリが表示されます。
static	（任意）**neighbor** コマンドを使用してスタティックに定義された EIGRP ネイバーを表示します。

デフォルト

インターフェイス名を指定しない場合、すべてのインターフェイスを介して学習されたネイバーが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp neighbors コマンドを使用して、ダイナミックに学習されたネイバーを EIGRP ネイバー テーブルからクリアできます。

static キーワードを使用しない限り、スタティック ネイバーは出力に含まれません。

例

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

```
hostname# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface       Holdtime Uptime   Q      Seq  SRTT  RTO
                                        (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1       13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0       14       0:02:01  0      10   12    24
```

```
172.16.80.31            Ethernet0     12        0:02:02  0       4     5      20
```

表 26-3 に、この出力で表示される重要なフィールドの説明を示します。

表 26-3　show eigrp neighbors のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。
Holdtime	セキュリティ アプライアンスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、セキュリティ アプライアンスは、ネイバーを到達不能と見なします。
Uptime	セキュリティ アプライアンスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
Q Count	セキュリティ アプライアンスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、セキュリティ アプライアンスがそのパケットの確認応答を受信するために必要なミリ秒数です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、セキュリティ アプライアンスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。

次に、**show eigrp neighbors static** コマンドの出力例を示します。

```
hostname# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

表 26-4 に、この出力で表示される重要なフィールドの説明を示します。

表 26-4　show ip eigrp neighbors static のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Static Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。

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

```
hostname# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)          (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

表 26-5 に、この出力で表示される重要なフィールドの説明を示します。

表 26-5　show ip eigrp neighbors details のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
H	このカラムは、指定されたネイバーとの間で確立されたピアリング セッションの順番を示します。順番は、0 から始まる連続した番号で指定されます。
Address	EIGRP ネイバーの IP アドレス。
Interface	セキュリティ アプライアンスがネイバーから hello パケットを受信するインターフェイス。
Holdtime	セキュリティ アプライアンスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。 ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。 この値が 0 に達すると、セキュリティ アプライアンスは、ネイバーを到達不能と見なします。
Uptime	セキュリティ アプライアンスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。
SRTT	スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、セキュリティ アプライアンスがそのパケットの確認応答を受信するために必要なミリ秒数です。
RTO	Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、セキュリティ アプライアンスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。
Q Count	セキュリティ アプライアンスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。
Seq Num	ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。
Version	指定されたピアが実行中のソフトウェア バージョン。
Retrans	パケットを再送した回数。

表 26-5　show ip eigrp neighbors details のフィールドの説明 （続き）

フィールド	説明
Retries	パケットの再送を試行した回数。
Restart time	指定されたネイバーが再起動してからの経過時間（時:分:秒）。

関連コマンド

コマンド	説明
clear eigrp neighbors	EIGRP ネイバー テーブルをクリアします。
debug eigrp neighbors	EIGRP ネイバー デバッグ メッセージを表示します。
debug ip eigrp	EIGRP パケット デバッグ メッセージを表示します。

show eigrp topology

EIGRP トポロジ テーブルを表示するには、特権 EXEC モードで **show eigrp topology** コマンドを使用します。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

構文の説明

active	（任意）EIGRP トポロジ テーブル内のアクティブ エントリのみ表示します。
all-links	（任意）EIGRP トポロジ テーブル内のすべてのルート（フィジブル サクセサでない場合も）を表示します。
as-number	（任意）EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
ip-addr	（任意）表示するトポロジ テーブルからの IP アドレス。マスクと一緒に指定した場合、エントリの詳細な説明が提供されます。
mask	（任意）*ip-addr* 引数に適用するネットワーク マスク。
pending	（任意）ネイバーからの更新を待機しているか、ネイバーへの応答を待機している、EIGRP トポロジ テーブル内のすべてのエントリを表示します。
summary	（任意）EIGRP トポロジ テーブルの要約を表示します。
zero-successors	（任意）EIGRP トポロジ テーブル内の使用可能なルートを表示します。

デフォルト

フィジブル サクセサであるルートのみが表示されます。**all-links** キーワードを使用すると、フィジブル サクセサでないものも含めたすべてのルートが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp topology コマンドを使用して、ダイナミック エントリをトポロジ テーブルから削除できます。

例

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

```
hostname# show eigrp topology
```

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.16.90.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.16.81.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

表 26-6 に、この出力で表示される重要なフィールドの説明を示します。

表 26-6　show eigrp topology のフィールド情報

フィールド	説明
Codes	このトポロジ テーブル エントリの状態。Passive および Active は、この宛先に関する EIGRP 状態を示し、Update、Query、および Reply は、送信中のパケットのタイプを示します。
P - Passive	ルートは良好だと認識され、この宛先についての EIGRP 計算は実行されません。
A - Active	この宛先についての EIGRP 計算が実行されます。
U - Update	この宛先に更新パケットが送信されたことを示します。
Q - Query	この宛先にクエリー パケットが送信されたことを示します。
R - Reply	この宛先に応答パケットが送信されたことを示します。
r - Reply status	ソフトウェアがクエリーを送信し、応答を待機しているときに設定されるフラグ。
address mask	宛先の IP アドレスとマスク。
successors	サクセサの数。この数値は、IP ルーティング テーブル内のネクストホップの数に対応します。「successors」が大文字で表示される場合、ルートまたはネクスト ホップは遷移状態です。
FD	フィジブル ディスタンス。フィジブル ディスタンスは、宛先に到達するための最適なメトリックか、ルートがアクティブだったときに認識された最適なメトリックです。この値はフィジビリティ条件チェックに使用されます。レポートされたルータのディスタンス（スラッシュの後のメトリック）がフィジブル ディスタンスより小さい場合、フィジビリティ条件が満たされて、そのパスはフィジブル サクセサになります。ソフトウェアによってパスがフィジブル サクセサだと判断されると、その宛先にクエリーを送信する必要はありません。
via	この宛先についてソフトウェアに通知したピアの IP アドレス。これらのエントリの最初の *n* 個（*n* はサクセサの数）は、現在のサクセサです。リスト内の残りのエントリはフィジブル サクセサです。
(*cost*/*adv_cost*)	最初の数値は宛先へのコストを表す EIGRP メトリックです。2 番めの数値はこのピアがアドバタイズした EIGRP メトリックです。
interface	情報の学習元のインターフェイス。

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は内部ルートについてのものです。

```
hostname# show eigrp topology 10.2.1.0 255.255.255.0
```

```
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は外部ルートについてのものです。

```
hostname# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

関連コマンド

コマンド	説明
clear eigrp topology	ダイナミックに検出されたエントリを EIGRP トポロジ テーブルからクリアします。

show eigrp traffic

送受信された EIGRP パケットの数を表示するには、特権 EXEC モードで **show eigrp traffic** コマンドを使用します。

show eigrp [*as-number*] **traffic**

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

clear eigrp traffic コマンドを使用すると、EIGRP トラフィックの統計情報をクリアできます。

例

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

```
hostname# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

表 26-7 に、この出力で表示される重要なフィールドの説明を示します。

表 26-7　show eigrp traffic のフィールドの説明

フィールド	説明
process	EIGRP ルーティング プロセスの自律システム番号です。
Hellos sent/received	送受信された hello パケットの数。
Updates sent/received	送受信された更新パケットの数。
Queries sent/received	送受信されたクエリー パケットの数。
Replies sent/received	送受信された応答パケットの数。
Acks sent/received	送受信された確認応答パケットの数。
Input queue high water mark/drops	最大受信しきい値に近づいている受信パケットの数と、ドロップされたパケットの数。
SIA-Queries sent/received	送受信されたアクティブ クエリーのスタック。
SIA-Replies sent/received	送受信されたアクティブ応答のスタック。

関連コマンド

コマンド	説明
debug eigrp packets	送受信された EIGRP パケットのデバッグ情報を表示します。
debug eigrp transmit	送信された EIGRP メッセージのデバッグ情報を表示します。

show failover

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

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

構文の説明

group	指定されたフェールオーバー グループの実行状態を表示します。
history	フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。履歴情報はデバイスをリブートするとクリアされます。
interface	フェールオーバー コマンドとステートフル リンクの情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー ユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ / スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。障害の理由が解消されても、障害の理由は出力に残ります。
statistics	フェールオーバー コマンド インターフェイスの送信および受信パケット数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。出力の情報が追加されました。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバー情報、インターフェイス ステータス、およびステートフル フェールオーバーの統計情報を表示します。Stateful Failover Logical Update Statistics 出力は、ステートフル フェールオーバーがイネーブルの場合のみ表示されます。「xerr」および「rerr」の値はフェールオーバーのエラーではなく、パケット送受信エラーの数を示します。

（注） ステートフル フェールオーバーは、ASA 5505 セキュリティ アプライアンスでは使用できません。したがって、ステートフル フェールオーバーの統計情報出力も使用できません。

show failover コマンド出力で、ステートフル フェールオーバーの各フィールドには次の値があります。

- Stateful Obj の値は次のとおりです。
  - xmit：送信されたパケットの数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケットの数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定のオブジェクト スタティック カウントを表します。
  - General：すべてのステートフル オブジェクトの合計を示します。
  - sys cmd：**login** または **stay alive** などの論理的なシステム更新コマンドを示します。
  - up time：セキュリティ アプライアンスのアップ タイムの値（アクティブなセキュリティ アプライアンスがスタンバイのセキュリティ アプライアンスに渡す）を示します。
  - RPC services：リモート プロシージャ コール接続情報。
  - TCP conn：ダイナミック TCP 接続情報。
  - UDP conn：ダイナミック UDP 接続情報。
  - ARP tbl：ダイナミック ARP テーブル情報。
  - Xlate_Timeout：接続変換タイムアウト情報を示します。
  - VPN IKE upd：IKE 接続情報。
  - VPN IPSEC upd：IPSec 接続情報。
  - VPN CTCP upd：cTCP トンネル接続情報。
  - VPN SDI upd：SDI AAA 接続情報。
  - VPN DHCP upd：トンネル型 DHCP 接続情報。
  - SIP Sesson：SIP シグナリング セッション情報。

フェールオーバー IP アドレスを入力しない場合、**show failover** コマンドでは IP アドレス 0.0.0.0 が表示され、インターフェイスのモニタリングは「waiting」状態のままになります。フェールオーバーを機能させるにはフェールオーバー IP アドレスを設定する必要があります。

表 26-8 に、フェールオーバーのインターフェイス状態の説明を示します。

表 26-8　フェールオーバー インターフェイス状態

状態	説明
Normal	インターフェイスは稼働中で、ピア ユニットの対応するインターフェイスから hello パケットを受信中です。
Normal (Waiting)	インターフェイスは稼働中ですが、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
Normal (Not-Monitored)	インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
No Link	物理リンクがダウンしています。

表 26-8　フェールオーバー インターフェイス状態 （続き）

状態	説明
No Link (Waiting)	物理リンクがダウンし、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。リンクが復元した後、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
No Link (Not-Monitored)	物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Link Down	物理リンクは動作中ですが、インターフェイスは管理上ダウンしています。
Link Down (Waiting)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスを動作状態にした後（インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを使用）、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
Link Down (Not-Monitored)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Testing	ピア ユニットの対応するインターフェイスから hello パケットが届かないため、インターフェイスはテスト モードです。
Failed	インターフェイスのテストに失敗し、インターフェイスは障害が発生したとしてマークされます。インターフェイスの障害によってフェールオーバー基準が満たされた場合、インターフェイスの障害によって、セカンダリ ユニットまたはフェールオーバー グループへのフェールオーバーが発生します。

マルチ コンフィギュレーション モードでは、**show failover** コマンドのみがセキュリティ コンテキストで使用でき、任意のキーワードを入力できません。

例

次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。セキュリティ アプライアンスは ASA 5500 シリーズのセキュリティ アプライアンスで、各セキュリティ アプライアンスのスロット 1 に詳細を示すように、それぞれ CSC SSM を装備しています。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
```

```
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3): Normal
                  Interface outside (10.132.9.3): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4): Normal
                  Interface outside (10.132.9.4): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

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

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

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

```
hostname# show failover

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

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

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
```

```
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

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

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

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

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

次に、ASA 5505 シリーズのセキュリティ アプライアンスでの **show failover** コマンドの出力例を示します。

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
```

```
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

次に、アクティブ-アクティブ セットアップでの **show failover state** コマンドの出力例を示します。

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

次に、アクティブ-スタンバイ セットアップでの **show failover state** コマンドの出力例を示します。

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 26-9 に、**show failover state** コマンドの出力の説明を示します。

表 26-9　show failover state の出力の説明

フィールド	説明
Configuration State	コンフィギュレーションの同期化の状態を表示します。 スタンバイ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing - STANDBY**：コンフィギュレーションの同期化が実行されているときに設定されます。 • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**：スタンバイ ユニットが、アクティブ ユニットとのコンフィギュレーションの同期化を完了したときに設定されます。 アクティブ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing**：スタンバイ ユニットに対してコンフィギュレーションの同期化を実行しているときにアクティブ ユニット上で設定されます。 • **Interface Config Syncing** • **Sync Done**：アクティブ ユニットが、スタンバイ ユニットに対してコンフィギュレーションの同期化を正常に完了したときに設定されます。 • **Ready for Config Sync**：スタンバイ ユニットがコンフィギュレーションの同期化を受信する準備が完了したという信号を送るときにアクティブ ユニット上で設定されます。
Communication State	MAC アドレスの同期化のステータスを表示します。 • **Mac set**：MAC アドレスがピア ユニットからこのユニットに同期化されました。 • **Updated Mac**：MAC アドレスが更新され、他のユニットに対して同期化する必要がある場合に使用されます。また、ユニットが遷移期間中に、ピア ユニットから同期化されたローカル MAC アドレスを更新する場合にも使用されます。
Date/Time	障害の日付およびタイムスタンプを表示します。
Last Failure Reason	最後にレポートされた障害の理由を表示します。この情報は、障害の条件が解消されてもクリアされません。この情報は、フェールオーバーが発生した場合にのみ変更されます。 可能な障害の理由は次のとおりです。 • **Ifc Failure**：障害が発生したインターフェイスの数がフェールオーバー基準を満たし、フェールオーバーが発生しました。 • **Comm Failure**：フェールオーバー リンクに障害が発生したか、ピアがダウンしています。 • **Backplane Failure**

表 26-9　show failover state の出力の説明 （続き）

フィールド	説明
State	ユニットの Primary/Secondary および Active/Standby ステータスを表示します。
This host/Other host	This host は、コマンドが実行されたデバイスについての情報を示します。Other host は、フェールオーバーのペアとなる他のデバイスについての情報を示します。

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

```
hostname# show failover history

==========================================================================
From State                To State                  Reason
==========================================================================
At   16:28:50 UTC Sep 9 2006
Not Detected              Negotiation               No Error

At   16:29:18 UTC Sep 9 2006
Negotiation               Cold Standby              Detected an Active mate

At   16:29:19 UTC Sep 9 2006
Cold Standby              Sync Config               Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync Config               Sync File System          Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync File System          Bulk Sync                 Detected an Active mate

At   16:29:36 UTC Sep 9 2006
Bulk Sync                 Standby Ready             Detected an Active mate

At   16:30:52 UTC Sep 9 2006
Standby Ready             Just Active               Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Just Active               Active Drain              Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Drain              Active Applying Config    Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Applying Config    Active Config Applied     Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Config Applied     Active                    Set by the CI config cmd

At   16:30:55 UTC Sep 9 2006
Active                    Disabled                  Set by the CI config cmd

==========================================================================
```

各エントリには、状態変更が発生した時刻および日付、開始状態、結果状態、および状態変更の理由が示されます。最も新しいエントリが表示の末尾に配置されます。古いエントリが上部に表示されます。最大で 60 エントリを表示できます。エントリが最大数に到達した場合、最も古いエントリが出力の上部から削除され、新しいエントリが末尾に追加されます。

表 26-10 に、フェールオーバーの状態を示します。状態には永続的と一時的の 2 つのタイプがあります。永続的な状態とは、障害などの何らかの出来事によって状態変更が発生するまで、ユニットが維持できる状態のことです。一時的な状態とは、ユニットが永続的な状態に到達するまでの間に経過する状態です。

表 26-10　フェールオーバーの状態

State	説明
Initialization	装置はプラットフォームの機能およびコンフィギュレーションをチェックし、フェールオーバー通信チャネルを準備しています。これは一時的なステートです。
Disabled	フェールオーバーはディセーブルです。これは安定したステートです。
Negotiation	ユニットはピアとの接続を確立し、ピアとネゴシエートして、ソフトウェア バージョンの互換性を判別し、Active/Standby ロールを決定します。ネゴシエートされたロールに基づき、ユニットはスタンバイ ユニット状態またはアクティブ ユニット状態になるか、障害状態になります。これは一時的なステートです。
Failed	ユニットは障害状態です。これは安定したステートです。
スタンバイ ユニット状態	
Cold Standby	ユニットはピアがアクティブ状態に到達するのを待機します。ピア ユニットがアクティブ状態に到達すると、このユニットは Standby Config 状態に進みます。これは一時的なステートです。
Sync Config	ユニットはピア ユニットから実行コンフィギュレーションを要求します。コンフィギュレーションの同期化中にエラーが発生した場合、ユニットは初期化状態に戻ります。これは一時的なステートです。
Sync File System	ユニットはピア システムとファイル システムを同期化します。これは一時的なステートです。
Bulk Sync	ユニットはピアから状態情報を受信します。この状態は、ステートフル フェールオーバーがイネーブルの場合にのみ発生します。これは一時的なステートです。
Standby Ready	ユニットは、アクティブ ユニットに障害が発生した場合に引き継ぐ準備が完了しています。これは安定したステートです。
アクティブ ユニット状態	
Just Active	ユニットがアクティブ ユニットになったときの最初の状態です。この状態にあるとき、ユニットがアクティブになること、および IP アドレスと MAC アドレスをインターフェイスに設定することをピアに通知するメッセージがピアに送信されます。これは一時的なステートです。
Active Drain	ピアからのキュー メッセージが廃棄されます。これは一時的なステートです。
Active Applying Config	ユニットはシステム コンフィギュレーションを適用します。これは一時的なステートです。
Active Config Applied	ユニットはシステム コンフィギュレーションの適用を完了しました。これは一時的なステートです。
Active	ユニットはアクティブで、トラフィックを処理しています。これは安定したステートです。

それぞれの状態変更の後に状態変更の理由が続きます。この理由は、ユニットが一時的な状態から永続的な状態に進んでも、通常同じままになります。次に、可能性がある状態変更の理由を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他のユニットのソフトウェア バージョンが異なっている
- 他のユニットの動作モードが異なっている
- 他のユニットのライセンスが異なっている
- 他のユニットのシャーシ コンフィギュレーションが異なっている
- 他のユニットのカード コンフィギュレーションが異なっている
- 他のユニットからアクティブ状態を要求された
- 他のユニットからスタンバイ状態を要求された
- 他のユニットが、このユニットに障害があるとレポートした
- 他のユニットが、そのユニットに障害があるとレポートした
- コンフィギュレーションの不一致
- アクティブ ユニットが検出された
- アクティブ ユニットが検出されなかった
- コンフィギュレーションの同期化が行われた
- 通信障害から回復した
- 他のユニットの VLAN コンフィギュレーションが異なっている
- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- このユニットの通信が失敗した
- フェールオーバー メッセージの ACK を受信しなかった
- 同期後の学習状態で他のユニットが動作しなくなった
- ピアの電源が検出されない
- フェールオーバー ケーブルがない
- HA 状態の進行に失敗した
- サービス カード障害が検出された
- 他のユニットのサービス カードに障害が発生した
- このユニットのサービス カードはピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア ユニットがリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーション同期化の状態を確認できない
- 自動更新要求

- 原因不明

関連コマンド

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

show failover exec

指定したユニットの **failover exec** コマンド モードを表示するには、特権 EXEC モードで **show failover exec** コマンドを使用します。

show failover exec {**active** | **standby** | **mate**}

構文の説明

active	アクティブ ユニットの **failover exec** コマンド モードを表示します。
mate	ピア ユニットの **failover exec** コマンド モードを表示します。
standby	スタンバイ ユニットの **failover exec** コマンド モードを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

failover exec コマンドは、指定したデバイスとのセッションを確立します。デフォルトでは、このセッションはグローバル コンフィギュレーション モードです。このセッションのコマンド モードは、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信することによって変更できます。指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。

show failover exec コマンドは、**failover exec** コマンドで送信されるコマンドが実行される、指定したデバイス上のコマンド モードを表示します。

例

次に、**show failover exec** コマンドの出力例を示します。この例では、**failover exec** コマンドが入力されるユニットのコマンド モードが、コマンドが実行される **failover exec** コマンド モードと同じである必要がないことを示しています。

この例では、スタンバイ ユニットにログインした管理者が、アクティブ ユニット上のインターフェイスに名前を追加します。この例で、**show failover exec mate** コマンドを 2 回めに入力したとき、ピア デバイスはインターフェイス コンフィギュレーション モードであると表示されます。**failover exec** コマンドでデバイスに送信されるコマンドは、このモードで実行されます。

```
hostname(config)# show failover exec mate
```

```
Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
hostname(config)# failover exec mate interface GigabitEthernet0/1
hostname(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
hostname(config)# failover exec mate nameif test
```

関連コマンド

コマンド	説明
failover exec	フェールオーバー ペアの指定されたユニット上で、入力されたコマンドを実行します。

show file

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

show file descriptors | system | information *filename*

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ファイル システム情報を表示する例を示します。

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

関連コマンド

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

show firewall

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

show firewall

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show firewall** コマンドの出力例を示します。

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

関連コマンド

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

show flash

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

show flash:

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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例は、内部フラッシュ メモリの内容を表示する方法を示しています。

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

```
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

関連コマンド

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

show fragment

IP フラグメント再構築モジュールの動作データを表示するには、特権 EXEC モードで **show fragment** コマンドを使用します。

show fragment [*interface*]

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データと動作データを分けるために、**show fragment** および **show running-config fragment** の 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データを表示する方法の例を示します。

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

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。

コマンド	説明
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show gc

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

show gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show gc** コマンドの出力例を示します。

```
hostname# show gc

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

関連コマンド

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

show h225

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

show h225

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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

show h225、**show h245**、または **show h323-ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。セッション レコードが多いときに **pager** コマンドが設定されていない場合、**show** コマンドの出力が末端に届くまでに時間がかかる場合があります。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

例

次に、**show h225** コマンドの出力例を示します。

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

この出力は、ローカル エンドポイント 10.130.56.3 と外部ホスト 172.30.254.203 との間でセキュリティ アプライアンスを通過するアクティブな H.323 コールが 1 つ存在し、これらのエンドポイントの間には、コールの CRV（Call Reference Value）が 9861 の同時コールが 1 つ存在することを示しています。

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

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h245

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

show h245

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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

例

次に、**show h245** コマンドの出力例を示します。

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

セキュリティ アプライアンスでアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。（TKTP ヘッダーは、各 H.225/H.245 メッセージの先頭の 4 バイト ヘッダーです。このヘッダーは、4 バイト ヘッダーを含むメッセージの長さを指定します）。外部ホスト エンドポイントは 172.30.254.203 で、TPKT 値が 0 のため、このエンドポイントからの次のパケットが TPKT ヘッダーを持つことが予想されます。

これらのエンドポイント間でネゴシエートされるメディアは、Logical Channel Number（LCN; 論理チャネル番号）が 258 で、外部の RTP IP アドレス / ポート ペアが 172.30.254.203/49608、RTCP IP アドレス / ポートが 172.30.254.203/49609、ローカルの RTP IP アドレス / ポート ペアが 10.130.56.3/49608、RTCP ポートが 49609 です。

値が 259 の 2 番めの LCN は、外部の RTP IP アドレス / ポート ペアが 172.30.254.203/49606、RTCP IP アドレス / ポート ペアが 172.30.254.203/49607、ローカルの RTP IP アドレス / ポート ペアが 10.130.56.3/49606、RTCP ポートが 49607 です。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h323-ras

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

show h323-ras

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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

show h323-ras コマンドは、H.323 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ための接続情報を表示し、**inspect protocol h323 {h225 | ras}** コマンド ページに説明されています。

例

次に、**show h323-ras** コマンドの出力例を示します。

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

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

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show history

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

show history

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show history コマンドを使用すると、以前入力したコマンドを表示できます。上矢印と下矢印を使用してコマンドを個別に調べて、**^p** を入力して以前に入力した行を表示するか、**^n** を入力して次の行を表示できます。

例

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

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

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

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

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

```
hostname(config)# show history
    show history
```

```
help
show history
enable
show history
config t
show history
```

関連コマンド

コマンド	説明
help	指定したコマンドのヘルプ情報を表示します。

show icmp

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

show icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

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

例

次に、ICMP コンフィギュレーションを表示する例を示します。

```
hostname# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

Interface Descriptor Block のステータスについての情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

show idb

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IDB はインターフェイス リソースを表す内部データ構造です。出力表示の詳細については、「例」を参照してください。

例

次に、**show idb** コマンドの出力例を示します。

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

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

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

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
```

```
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

表 26-11 に、各フィールドの説明を示します。

表 26-11　show idb stats の各フィールド

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

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
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 igmp groups

セキュリティ アプライアンスに直接接続された受信者、および IGMP によって学習された受信者を含むマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

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

構文の説明

detail	（任意）ソースの詳細説明を出力します。
group	（任意）IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。
if_name	（任意）指定されたインターフェイスについてのグループ情報を表示します。
reserved	（任意）予約されたグループについての情報を表示します。
summary	（任意）グループ加入の要約情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたマルチキャスト グループを、グループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

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

```
hostname#show igmp groups

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

関連コマンド

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

show igmp interface

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

show igmp interface [*if_name*]

構文の説明

if_name	（任意）選択したインターフェイスについての IGMP グループ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。**detail** キーワードが削除されました。

使用上のガイドライン

オプションの *if_name* 引数を省略すると、**show igmp interface** コマンドはすべてのインターフェイスについての情報を表示します。

例

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

```
hostname# show igmp interface inside

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

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。

show igmp traffic

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

show igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

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

```
hostname# show igmp traffic

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

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

関連コマンド

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

show import webvpn

セキュリティ アプライアンスのフラッシュ メモリに現在存在する WebVPN カスタム データとプラグインをリストするには、特権 EXEC モードで **show import webvpn**（*任意*）コマンドを入力します。

show import webvpn | customization | plug-in | plug-in detail | translation-table | url-list | webcontent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show import webvpn コマンドを使用すると、WebVPN ユーザが使用可能なカスタム データおよび Java ベースのクライアント アプリケーションが識別されます。表示されるリストでは、セキュリティ アプライアンスのフラッシュ メモリにある要求されるすべてのデータ タイプの詳細が表示されます。

それぞれの show import webvpn コマンドでは、次に示す現在ロードされている WebVPN データが表示されます。

- カスタマイゼーション：カスタマイゼーション オブジェクト（ファイル名は base64 でデコード）
- プラグイン：サード パーティ製 Java ベースのクライアント アプリケーション（SSH、VNC、および RDP）
- プラグインの詳細情報：各プラグインのハッシュ情報と日付情報
- 変換テーブル：ローカリゼーションおよび国際化辞書テーブル
- URL リスト：URL リスト オブジェクト（ファイル名は base64 でデコード）
- Web コンテンツ：再帰的な disk0:/csco_config/htms（すべてのファイルのフルネーム）

例

次に、さまざまな **show import webvpn** コマンドによって表示される WebVPN データの例を示します。

```
hostname# show import webvpn plug-in
ssh
rdp
```

```
vnc
hostname#

hostname# show import webvpn customization
Template
DfltCustomization
hostname#

hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
hostname#

hostname# show import webvpn url-list
Template
No bookmarks are currently defined
hostname#

hostname# show import webvpn webcontent
No custom webcontent is loaded
hostname#
```

関連コマンド

コマンド	説明
revert webvpn all	セキュリティ アプライアンスに現在存在するすべての WebVPN データおよびプラグインを削除します。

show interface

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

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [**stats** | **detail**]

構文の説明

detail	（任意）インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態、非対称ルーティングの統計情報（**asr-group** コマンドによって非対称ルーティングがイネーブルになっている場合）が含まれます。すべてのインターフェイスを表示する場合、SSM 用の内部インターフェイスが ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールされているとき、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabitethernet 0/1** のようなインターフェイス ID を識別します。有効値については、**interface** コマンドを参照してください。
redundant*number*	（任意）**redundant1** のような冗長インターフェイス ID を識別します。
stats	（デフォルト）インターフェイス情報および統計情報を表示します。このキーワードはデフォルトであるため、このキーワードはオプションです。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

いずれのオプションも識別しない場合、このコマンドはすべてのインターフェイスについての基本的な統計情報を表示します。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいインターフェイス番号付け方式を取り入れるように変更され、明示的に指定するための **stats** キーワード、および **detail** キーワードが追加されました。
7.0(4)	このコマンドに、4GE SSM インターフェイス用のサポートが追加されました。
7.2(1)	このコマンドに、スイッチ インターフェイス用のサポートが追加されました。
8.0(2)	このコマンドに、冗長インターフェイス用のサポートが追加されました。また、サブインターフェイス用の遅延が追加されました。入力リセット ドロップと出力リセット ドロップの 2 つの新しいカウンタが追加されました。

使用上のガイドライン

1 つのインターフェイスが複数のコンテキストで共有されているときに、あるコンテキストでこのコマンドを入力した場合、セキュリティ アプライアンスは現在のコンテキストの統計情報だけを表示します。物理インターフェイスのシステム実行スペース内でこのコマンドを使用すると、セキュリティ アプライアンスはすべてのコンテキストについて組み合わせた統計情報を表示します。

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

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

（注） Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

ハードウェア カウントでは、トラフィック量はハードウェアから直接取得され、レイヤ 2 のパケットサイズが反映されます。一方、Traffic Statistics では、レイヤ 3 パケットのサイズが反映されます。

カウントの差はインターフェイス カード ハードウェアの設計に基づいて異なります。

たとえば、ファスト イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーを含むため、トラフィック カウントよりも 14 バイト大きくなります。ギガビット イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーと CRC の両方を含むため、トラフィック カウントよりも 18 バイト大きくなります。

出力表示の詳細については、「例」を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
hostname# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
```

```
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
```

```
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
```

```
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

表 26-12 に、各フィールドの説明を示します。

表 26-12　show interface のフィールド

フィールド	説明
Interface *ID*	インターフェイス ID。コンテキスト内では、**allocate-interface** コマンドで **visible** キーワードを設定しない限り、セキュリティ アプライアンスはマッピング名（設定されている場合）を表示します。
"*interface_name*"	**nameif** コマンドで設定されたインターフェイス名。システム実行スペースでは、システムに名前を設定できないため、このフィールドはブランクです。名前を設定しない場合、Hardware 行の下に次のメッセージが表示されます。 `Available but not configured via nameif`
is *state*	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Line protocol is *state*	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。
VLAN identifier	サブインターフェイスの場合、VLAN ID。
Hardware	インターフェイスのタイプ、最大帯域幅、遅延、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコで囲まれて設定値とともに表示されます。次に、一般的なハードウェア タイプを示します。 • i82542：PIX プラットフォームで使用される Intel PCI ファイバ ギガビット カード • i82543：PIX プラットフォームで使用される Intel PCI-X ファイバ ギガビット カード • i82546GB：ASA プラットフォーム上で使用される Intel PCI-X 銅線ギガビット • i82547GI：ASA プラットフォーム上でバックプレーンとして使用される Intel CSA 銅線ギガビット • i82557：ASA プラットフォーム上で使用される Intel PCI 銅線ファスト イーサネット • i82559：PIX プラットフォームで使用される Intel PCI 銅線ファスト イーサネット • VCS7380：SSM-4GE で使用される Vitesse 4 ポート ギガビット スイッチ

表 26-12　show interface のフィールド （続き）

フィールド	説明
Media-type	（4GE SSM インターフェイスの場合のみ）インターフェイスが RJ-45 または SFP のいずれとして設定されているかを示します。

message area	一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。
	• システム実行スペースで、次のメッセージが表示される場合があります。
	`Available for allocation to a context`
	• 名前を設定しない場合、次のメッセージが表示されます。
	`Available but not configured via nameif`
	• インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。
	`Active member of Redundant5`

MAC address	インターフェイスの MAC アドレス。
MTU	このインターフェイス上で許可されるパケットの最大サイズ（バイト単位）。インターフェイス名を設定しない場合、このフィールドには「MTU not set」と表示されます。
IP address	**ip address** コマンドを使用して設定したか、DHCP サーバから受信したインターフェイスの IP アドレス。システム実行スペースでは、システムに IP アドレスを設定できないため、このフィールドには「IP address unassigned」と表示されます。
Subnet mask	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信したパケットの数。
Bytes	このインターフェイスで受信したバイト数。
No buffer	メイン システムのバッファ スペースがなかったために、廃棄された受信済みパケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
Received:	
Broadcasts	受信したブロードキャストの数。
Input errors	次に示すタイプを含めた入力エラーの総数。入力に関係する他のエラーも入力エラーのカウントが増加する原因になります。また、一部のデータグラムは複数のエラーを含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。
Runts	最小のパケット サイズ（64 バイト）よりも小さいために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。
Giants	最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

表 26-12　show interface のフィールド （続き）

フィールド	説明
CRC	Cyclical Redundancy Check（CRC; 巡回冗長検査）エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、セキュリティ アプライアンスは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。
Frame	フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。
Overrun	セキュリティ アプライアンスのデータ処理能力を入力レートが超えたため、セキュリティ アプライアンスがハードウェア バッファに受信したデータを処理できなかった回数。
Ignored	このフィールドは使用されません。値は常に 0 です。
Abort	このフィールドは使用されません。値は常に 0 です。
L2 decode drops	名前がまだ設定されていないか（**nameif** コマンド）、無効な VLAN ID を持つフレームが受信されたためにドロップしたパケットの数。
Packets output	このインターフェイスに送信されたパケットの数。
Bytes	このインターフェイスに送信されたバイトの数。
Underruns	セキュリティ アプライアンスが処理できるよりも速くトランスミッタが稼働した回数。
Output Errors	設定されたコリジョンの最大数を超えたため送信されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。
Collisions	イーサネット コリジョン（単一および複数のコリジョン）が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスで 3 秒間送信できない場合、セキュリティ アプライアンスはインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。インターフェイスのリセットは、インターフェイスがループバックまたはシャットダウンする場合も発生します。
Babbles	未使用。（「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します）。

表 26-12　show interface のフィールド （続き）

フィールド	説明
Late collisions	通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。 レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、セキュリティ アプライアンスはパケットの送信を部分的に完了しています。セキュリティ アプライアンスは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で送信前に保留されたフレームの数。
input reset drops	リセットが発生したときに RX リングでドロップしたパケットの数をカウントします。
output reset drops	リセットが発生したときに TX リングでドロップしたパケットの数をカウントします。
Rate limit drops	（4GE SSM インターフェイスの場合だけ）ギガビット以外の速度でインターフェイスを設定して、設定に応じて 10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。
Lost carrier	送信中に搬送波信号が消失した回数。
No carrier	未使用。
Input queue (curr/max packets):	入力キュー内のパケットの数（現行値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。ギガビット イーサネット インターフェイスでは使用できません。
Output queue (curr/max packets):	出力キュー内のパケットの数（現行値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Traffic Statistics:	受信、送信、またはドロップしたパケットの数。
Packets input	受信したパケットの数とバイトの数。
Packets output	送信したパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。このカウンタは通常、Accelerated Security Path（ASP; 高速セキュリティ パス）上でドロップしたパケットについて増分します（たとえば、アクセス リスト拒否が原因でパケットをドロップした場合など）。 インターフェイス上でドロップが発生する原因については、**show asp drop** コマンドを参照してください。

表 26-12　show interface のフィールド （続き）

フィールド	説明
1 minute input rate	過去 1 分間に受信したパケットの数（パケット / 秒およびバイト / 秒）。
1 minute output rate	過去 1 分間に送信したパケットの数（パケット / 秒およびバイト / 秒）。
1 minute drop rate	過去 1 分間にドロップしたパケットの数（パケット / 秒）。
5 minute input rate	過去 5 分間に受信したパケットの数（パケット / 秒およびバイト / 秒）。
5 minute output rate	過去 5 分間に送信したパケットの数（パケット / 秒およびバイト / 秒）。
5 minute drop rate	過去 5 分間にドロップしたパケットの数（パケット / 秒）。
Redundancy Information:	冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブ インターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。 メンバーをまだ割り当てていない場合、次の出力が表示されます。 `Members unassigned`
Last switchover	冗長インターフェイスの場合、アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした時刻を表示します。

次に、スイッチ ポートを含む ASA 5505 適応型セキュリティ アプライアンス上での **show interface** コマンドの出力例を示します。

```
hostname# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

表 26-13 に、ASA 5505 適応型セキュリティ アプライアンスのスイッチ インターフェイスなどのスイッチ インターフェイスに対する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 26-1 を参照してください。

表 26-13　スイッチ インターフェイスの show interface のフィールド

フィールド	説明
switch ingress policy drops	このドロップは通常、ポートが正しく設定されていないときに表示されます。このドロップは、デフォルトまたはユーザ設定のスイッチ ポート設定の結果としてスイッチ ポート内でパケットが正常に転送できない場合に増分されます。このドロップの原因として、次のコンフィギュレーションが考えられます。 • **nameif** コマンドが VLAN インターフェイス上で設定されていない。 **（注）** 同じ VLAN 内のインターフェイスに、**nameif** コマンドが設定されていなかった場合でも、VLAN 内のスイッチングは正常で、このカウンタは増分されません。 • VLAN がシャットダウンしている。 • アクセス ポートで 802.1Q タグが付いたパケットを受信した。 • トランク ポートで許可されないタグまたはタグのないパケットを受信した。 • セキュリティ アプライアンスが、イーサネット キープアライブを持つ別のシスコ デバイスに接続されている。たとえば、Cisco IOS ソフトウェアではインターフェイス ヘルス状態を確認するためにイーサネット ループバック パケットを使用します。このパケットは、他のデバイスによって受信されるためのものではなく、パケットをただ送信できることによって、ヘルス状態が確認されます。これらのタイプのパケットはスイッチ ポートでドロップされ、カウンタが増分されます。 • VLAN に物理インターフェイスが 1 つしか存在しないが、パケットの DEST は VLAN の MAC アドレスと一致せず、ブロードキャスト アドレスでない。
switch egress policy drops	現在使用されていません。

次に、**show interface detail** コマンドの出力例を示します。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（**asr-group** コマンドでイネーブルにされている場合）を表示する例を示します。

```
hostname# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
```

```
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 26-14 に、**show interface detail** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 26-1 を参照してください。

表 26-14　show interface detail の各フィールド

フィールド	説明
Demux drops	(内部データ インターフェイスのみ) セキュリティ アプライアンスが SSM インターフェイスからのパケットを逆多重化できなかったためドロップしたパケットの数。SSM インターフェイスはバックプレーンを介してネイティブ インターフェイスと通信し、すべての SSM インターフェイスからのパケットはバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	デバッグに使用される 0 から始まる番号で、このインターフェイスが作成された順番を示します。
Interface config status	管理ステートは次のとおりです。 • active：インターフェイスはシャット ダウンされていません。 • not active：インターフェイスは **shutdown** コマンドでシャット ダウンされています。
Interface state	インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。ハイ アベイラビリティに設定した場合、セキュリティ アプライアンスは必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信した ASR パケットの数。

表 26-14　show interface detail の各フィールド （続き）

フィールド	説明
Transmitted X2 packets	このインターフェイスで送信した ASR パケットの数。
Dropped X3 packets	このインターフェイスでドロップした ASR パケットの数。パケットは、パケットを転送しようとしたときにインターフェイスがダウン状態の場合にドロップされることがあります。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
delay	インターフェイスの遅延メトリックを変更します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

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

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

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドでは、VLAN インターフェイス、およびトランスペアレント モードでの管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。

使用上のガイドライン

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

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip brief** コマンドの出力例を示します。

```
hostname# show interface ip brief
```

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

表 26-15 に、各フィールドの説明を示します。

表 26-15　show interface ip brief の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。すべてのインターフェイスを表示する場合、AIP SSM の内部インターフェイスに関する情報が表示されます（ASA 適応型セキュリティ アプライアンスに取り付けられている場合）。内部インターフェイスは、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
IP-Address	インターフェイスの IP アドレス。
OK?	このカラムは現在使用されておらず、常に「Yes」と表示されます。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。
Status	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Protocol	回線ステータスは次のとおりです。 • up：動作するケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show inventory

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

show inventory [**slot**]

構文の説明

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

デフォルト

インベントリを表示するスロットを指定しない場合は、次のように処理されます。

- 電源を含めて、すべての SSM のインベントリ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	セマンティックに小さな変更が加えられました。

使用上のガイドライン

show inventory コマンドを使用すると、各シスコ製品に関するインベントリ情報が取得され、UDI 形式で表示されます。UDI は、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）という 3 つの別個のデータ要素を結合したものです。

PID は、製品の注文に使用する名前です。歴史的には、「製品名」または「部品番号」と呼ばれていました。これは、正確な交換部品を注文するために使用する ID です。

VID は製品のバージョンです。製品が改訂されるたびに、VID は増加します。VID は、製品変更の通知を管理する業界のガイドラインである、Telcordia GR-209-CORE から取得された厳格なプロセスに従って増加されます。

SN はベンダー固有の製品の通し番号です。それぞれの製造済み製品には、現場では変更できない固有のシリアル番号が工場で割り当てられます。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

UDI では各製品をエンティティと呼びます。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。各エンティティは、シスコ エンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワーキング デバイスに取り付けられており、PID が割り当てられているシスコ エンティティのリストが表示されます。

例

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

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

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

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

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

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

表 26-16 は、この出力で表示されるフィールドについて説明しています。

表 26-16　show inventory フィールドの説明

フィールド	説明
Name	シスコ エンティティに割り当てられた物理名（テキスト ストリング）。たとえば、デバイスの物理コンポーネント命名構文に応じた「1」などのコンソールまたは簡易コンポーネントの番号（ポートまたはモジュールの番号）。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトを特徴付けるシスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。
VID	エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	エンティティのシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

関連コマンド

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

show ip address

インターフェイス IP アドレス（トランスペアレント モードの場合は管理 IP アドレス）を表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

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

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

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

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドに、VLAN インターフェイス用のサポートが追加されました。

使用上のガイドライン

このコマンドは、ハイ アベイラビリティに設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

例

次に、**show ip address** コマンドの出力例を示します。

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

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

表 26-17 に、各フィールドの説明を示します。

表 26-17　show ip address の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。
Name	**nameif** コマンドで設定されたインターフェイス名。
IP address	インターフェイスの IP アドレス。
Subnet mask	IP アドレスのサブネット マスク。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

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

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

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
server	DHCP サーバに関する情報を表示します。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいサーバ機能に対応するように **lease** および **server** キーワードが追加されました。
7.2(1)	このコマンドでは、VLAN インターフェイス、およびトランスペアレント モードでの管理 0/0 インターフェイスまたはサブインターフェイスのサポートが追加されました。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

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

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
```

```
DHCP Transaction id:0x4123
Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
Temp default-gateway addr:209.165.201.1
Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
Next timer fires after:111797 secs
Retry count:0, Client-ID:cisco-0000.0000.0000-outside
Proxy: TRUE  Proxy Network: 10.1.1.1
Hostname: device1
```

表 26-18 に、各フィールドの説明を示します。

表 26-18　show ip address dhcp lease の各フィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネット マスク。
DHCP Lease server	DHCP サーバ アドレス。
state	DHCP リースの状態で、次のとおりです。 • [Initial]：初期化状態で、セキュリティ アプライアンスがリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。 • [Selecting]：セキュリティ アプライアンスは 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。 • [Requesting]：セキュリティ アプライアンスは、要求を送信した送信先サーバからの応答を待機しています。 • Purging：クライアントが IP アドレスを解放したか、他のエラーが発生したため、セキュリティ アプライアンスはリースを削除します。 • [Bound]：セキュリティ アプライアンスは有効なリースを保持し、正常に動作しています。 • [Renewing]：セキュリティ アプライアンスはリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。 • [Rebinding]：セキュリティ アプライアンスは元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。 • [Holddown]：セキュリティ アプライアンスはリースを削除するプロセスを開始しました。 • [Releasing]：セキュリティ アプライアンスは IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。
DHCP transaction id	クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバによって使用される乱数。
Lease	DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。

表 26-18　show ip address dhcp lease の各フィールド （続き）

フィールド	説明
Rebind	セキュリティ アプライアンスが DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、セキュリティ アプライアンスが元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。セキュリティ アプライアンスは、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
Temp default-gateway addr	DHCP サーバによって指定されるデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルト スタティック ルート。
Next timer fires after	内部タイマーがトリガーするまでの秒数。
Retry count	セキュリティ アプライアンスがリースを設定しようとしているとき、このフィールドは、セキュリティ アプライアンスが DHCP メッセージの送信を試行した回数を示します。たとえば、セキュリティ アプライアンスが Selecting 状態の場合、この値はセキュリティ アプライアンスが探索メッセージを送信した回数を示します。セキュリティ アプライアンスが Requesting 状態の場合、この値はセキュリティ アプライアンスが要求メッセージを送信した回数を示します。
Client-ID	サーバとのすべての通信に使用したクライアント ID。
Proxy	このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

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

```
hostname# show ip address outside dhcp server

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

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

表 26-19 に、各フィールドの説明を示します。

表 26-19　show ip address dhcp server の各フィールド

フィールド	説明
DHCP server	このインターフェイスがリースを取得した DHCP サーバ アドレス。最上位エントリ（「ANY」）はデフォルト サーバで常に存在します。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は一般的に 1 です。VPN 用のプロキシを実行中のインターフェイスに対してサーバがアドレスを提供している場合、リースは複数となります。
Offers	サーバからのオファーの数。
Requests	サーバに送信された要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した拒否の数。
Releases	サーバに送信されたリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバ アドレス。
DNS1	DHCP サーバから取得したセカンダリ DNS サーバ アドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバ アドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバ アドレス。
Subnet	DHCP サーバから取得したサブネット アドレス。
DNS Domain	DHCP サーバから取得したドメイン。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address dhcp	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、特権 EXEC モードで **show ip address pppoe** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、VLAN インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

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

出力表示の詳細については、「例」を参照してください。

例

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

```
hostname# show ip address outside pppoe
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address ppoe	PPPoE サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

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

構文の説明

global	（デフォルト）すべてのインターフェイスについての一致数を表示します。
interface *interface_name*	（任意）指定したインターフェイスについての一致数を表示します。

デフォルト

キーワードを指定しない場合、このコマンドは、すべてのインターフェイスについての一致数を表示します（**global**）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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

例

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

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

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

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

関連コマンド

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

show ip verify statistics

ユニキャスト RPF 機能が原因でドロップしたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。ユニキャスト RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

show ip verify statistics [interface *interface_name*]

構文の説明

interface *interface_name*	（任意）指定したインターフェイスの統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

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

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

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ips

AIP SSM で設定されている使用可能な IPS 仮想センサーをすべて表示するには、特権 EXEC モードで **show ips** コマンドを使用します。

show ips [**detail**]

構文の説明

detail	（任意）センサーの ID 番号と名前を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

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、システム実行スペースで入力するとすべての仮想センサーを表示しますが、コンテキスト実行スペース内ではコンテキストに割り当てられた仮想センサーのみ表示します。仮想センサーをコンテキストに割り当てることについては、**allocate-ips** コマンドを参照してください。

仮想センサーは IPS バージョン 6.0 以降で使用できます。

例

次に、**show ips** コマンドの出力例を示します。

```
hostname# show ips
Sensor name
------------
ips1
ips2
```

次に、**show ips detail** コマンドの出力例を示します。

```
hostname# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
ips	トラフィックを AIP SSM に迂回させます。

show ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。また、このコマンドの代替形式の **show crypto ipsec sa** も使用できます。

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

構文の説明

detail	（任意）表示されているものに対する詳細なエラー情報を表示します。
entry	（任意）IPSec SA をピア アドレスの順に表示します。
identity	（任意）IPSec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	（任意）指定されたクリプト マップの IPSec SA を表示します。
peer *peer-addr*	（任意）指定されたピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec SA が表示されます。

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

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

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

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

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

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

    Crypto map tag: def, local addr: 10.132.0.17

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

（注） IPSec SA ポリシーに、フラグメンテーションは IPSec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーで、フラグメンテーションは IPSec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次の例をグローバル コンフィギュレーション モードで入力すると、def という名前のクリプト マップの IPSec SA が表示されます。

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

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

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

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

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

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
```

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

    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

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

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry** に対する IPSec SA が表示されます。

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

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

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

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

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

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

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

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

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

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

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

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

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry detail** を使って、IPSec SA が表示されます。

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

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

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

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

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

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

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

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

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

```
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

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

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

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

次に、キーワード **identity** を使った IPSec SA の例を示します。

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

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

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

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

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

    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

次に、キーワード **identity** および **detail** を使った IPSec SA の例を示します。

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

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

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

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

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

    Crypto map tag: def, local addr: 172.20.0.17

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

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

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

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

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

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

show ipsec sa summary

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IPSec SA の要約を次の接続タイプ別に表示する例を示します（グローバル コンフィギュレーション モードで入力）。

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

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

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

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA を完全に削除するか、特定のパラメータに基づいて削除します。
show ipsec sa	IPSec SA のリストを表示します。
show ipsec stats	IPSec 統計情報のリストを表示します。

show ipsec stats

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

show ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
IPsec Global Statistics	このセクションは、セキュリティ アプライアンスがサポートする IPsec トンネルの総数に関係します。
Active tunnels	現在接続されている IPsec トンネルの数。
Previous tunnels	接続されたことがある IPsec トンネルの数（アクティブなトンネルを含む）。
Inbound	このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。
Bytes	受信した暗号トラフィックのバイト数。
Decompressed bytes	圧縮解除が実行された後に受信された暗号トラフィックのバイト数（該当する場合）。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	受信された IPsec 暗号化パケットの数。
Dropped packets	受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。

出力 （続き）	説明 （続き）
Replay failures	受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。
Authentications	受信された IPsec 暗号化パケットについて実行された認証の成功数。
Authentication failures	受信された IPsec 暗号化パケットについて検出された認証の失敗数。
Decryptions	受信された IPsec 暗号化パケットについて実行された復号化の成功数。
Decryption failures	受信された IPsec 暗号化パケットについて検出された復号の失敗数。
Decapsulated fragments needing reassembly	再構築が必要な IP フラグメントを含む復号 IPSec パケットの数。
Outbound	このセクションは、IPsec トラフィックを介して送信される発信クリアテキスト トラフィックに関係します。
Bytes	IPsec トンネルを介して暗号化および送信されるクリアテキスト トラフィックのバイト数。
Uncompressed bytes	IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキスト トラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	IPsec トンネルを介して暗号化および送信されるクリアテキスト パケットの数。
Dropped packets	IPsec トンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキスト パケットの数。
Authentications	IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。
Authentication failures	IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。
Encryptions	IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。
Encryption failures	IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。
Fragmentation successes	発信 IPsec パケットの変換の一部として実行されたフラグメンテーション操作の成功数。
Pre-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragmentation failures	発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。

出力 （続き）	説明 （続き）
Pre-fragmentation failures	発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation failure	発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragments created	IPsec の変換の一部として作成されたフラグメントの数。
PMTUs sent	IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。
PMTUs recvd	IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。
Protocol failures	受信した不正な形式の IPsec パケットの数。
Missing SA failures	指定された IPsec セキュリティ アソシエーションが存在しない、要求された IPsec の動作の数。
System capacity failures	IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できない IPsec の動作の数。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
```

```
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

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

show ipv6 access-list

IPv6 アクセス リストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセス リストは、セキュリティ アプライアンスを通過できる IPv6 トラフィックを決定します。

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

構文の説明

any	（任意）IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	（任意）特定のホストの IPv6 アドレス。指定した場合、指定されたホストについてのアクセス ルールのみが表示されます。
id	（任意）アクセス リストの名前。指定した場合、指定されたアクセス リストのみが表示されます。
source-ipv6-prefix /*prefix-length*	（任意）IPv6 ネットワーク アドレスおよびプレフィックス。指定した場合、指定された IPv6 ネットワークについてのアクセス ルールのみが表示されます。

デフォルト

すべての IPv6 アクセス リストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

例

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

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

```
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

関連コマンド

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

show ipv6 interface

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

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

構文の説明

brief	各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。
if_name	（任意）**nameif** コマンドで指定された内部または外部のインターフェイス名。指定されたインターフェイスのステータスおよびコンフィギュレーションのみが表示されます。
prefix	（任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。プレフィックスは、IPv6 アドレスのネットワーク部分です。

デフォルト

すべての IPv6 インターフェイスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 interface** コマンドの出力は **show interface** コマンドと類似しています。インターフェイスのハードウェアが使用できる場合、インターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

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

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
```

```
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

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

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

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

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

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

show ipv6 mld traffic

Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタ情報を表示するには、特権 EXEC モードで **show ipv6 mld traffic** コマンドを使用します。

show ipv6 mld traffic

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 mld traffic コマンドを使用すると、予期される数の MLD メッセージが受信および送信されたかどうかをチェックできます。

show ipv6 mld traffic コマンドで提供される情報は次のとおりです。

- **Elapsed time since counters cleared**：カウンタがクリアされてからの経過時間。
- **Valid MLD Packets**：受信および送信された有効な MLD パケットの数。
- **Queries**：受信および送信された有効なクエリーの数。
- **Reports**：受信および送信された有効なレポートの数。
- **Leaves**：受信および送信された有効な脱退の数。
- **Mtraee packets**：受信および送信されたマルチキャスト トレース パケットの数。
- **Errors**：発生したエラーのタイプと数。

例

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

```
hostname# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                   Received           Sent
Valid MLD Packets  1                  3
Queries            1                  0
```

```
Reports            0                  3
Leaves             0                  0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

関連コマンド

コマンド	説明
clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。

show ipv6 neighbor

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

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

構文の説明

address	（任意）指定された IPv6 アドレスについてのみネイバー探索キャッシュ情報を表示します。
if_name	（任意）**nameif** コマンドで設定する、指定されたインターフェイス名についてのみキャッシュ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 neighbor コマンドで提供される情報は次のとおりです。

- **IPv6 Address**：ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age**：アドレスが到達可能と確認されてからの経過時間（分単位）。ハイフン（-）はスタティック エントリを示します。
- **Link-layer Addr**：MAC アドレス。アドレスが不明の場合、ハイフン（-）が表示されます。
- **State**：ネイバー キャッシュ エントリの状態。

（注） 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、**INCMP**（不完全）状態と **REACH**（到達可能）状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

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

- **INCMP**：（不完全）エントリに対してアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。

- **REACH**：（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。**REACH** 状態になっている間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。
- **STALE**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。**STALE** 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。
- **DELAY**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。**DELAY** 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE**：到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認をアクティブに要求します。
- **????**：不明な状態。

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

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

- **Interface**

  アドレスに到達可能であったインターフェイス。

例

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

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

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

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

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
ipv6 neighbor	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

show ipv6 route

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

show ipv6 route

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 専用の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show route** コマンドと類似しています。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

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

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

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

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブル アップデートおよびルート キャッシュ アップデートのデバッグ メッセージを表示します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 routers

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

show ipv6 routers [*if_name*]

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

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

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

関連コマンド

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

show ipv6 traffic

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

show ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トラフィック カウンタをクリアするには、**clear ipv6 traffic** コマンドを使用します。

例

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

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

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

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

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

関連コマンド

コマンド	説明
clear ipv6 traffic	ipv6 トラフィック カウンタをクリアします。