show f ～ show ipu

show facility-alarm

ISA 3000 のトリガーされたアラームを表示するには、ユーザー EXEC モードで **show facility-alarm** コマンドを使用します。

show facility-alarm { **relay | status** [**info | major | minor**] }

構文の説明

relay	アラーム出力リレーを通電状態にしたアラームを表示します。
status [**info** | **major** | **minor**]	トリガーされたすべてのアラームを表示します。リストを制限するには、次のキーワードを追加します。 • **major**：すべてのメジャーシビラティ（重大度）のアラームが表示されます。 • **minor**：すべてのマイナーシビラティ（重大度）のアラームが表示されます。 • **info**：すべてのアラームが表示されます。このキーワードを使用すると、キーワードを使用しない場合と同じ出力になります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

アラーム出力リレーを通電したアラームだけを表示するには、**relay** キーワードを使用します。出力アラームリレーは、トリガーされたアラームを有効にするよう設定したかどうかに基づいて通電されます。アラーム出力リレーを通電すると、接続しているデバイス（点滅光やブザーなど）がアクティブになります。

アラームアクションが外部アラーム出力リレーをトリガーしたかどうかに関わらず、トリガーされたすべてのアラームを表示するには、**status** キーワードを使用します。

次の表は出力の列について示しています。

カラム	説明
ソース（Source）	アラームがトリガーされたデバイス。通常は、デバイスで設定されているホスト名です。
Severity	[Major] または [minor] です。
説明	トリガーされたアラームのタイプ。たとえば、温度、アラームの外部連絡先、冗長電源など。
Relay	外部アラーム出力リレーが通電または非通電のどちらであったか。外部出力アラームは、アラーム設定に基づいてトリガーされます。
時刻	トリガーされたアラームのタイムスタンプ。

例

次に、**show facility-alarm relay** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm relay

Source    Severity   Description                          Relay      Time
ciscoasa  minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
 22 2014
```

次に、**show facility-alarm status** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm status info

Source    Severity  Description                        Relay         Time
ciscoasa minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
22 2014
ciscoasa minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
22 2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa> show facility-alarm status major
Source    Severity  Description                       Relay         Time
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
 22 2014
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
 22 2014
ciscoasa> show facility-alarm status minor
Source    Severity  Description                         Relay         Time
ciscoasa  minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon
Sep 22 2014
ciscoasa  minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon
Sep 22 2014
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	入力アラーム コンタクトのステータスを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

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 [**descriptor**] [**exec**] [**group** *num* | **history** [**details**] | **interface** | **state** | **trace** [オプション] | [**statistics** [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync** [**all** | **control-plane** | **data-plane** |] | **interface** [**all**]] | **details**] [**config-sync**]

構文の説明

記述子	フェールオーバーインターフェイス記述子を、インターフェイスごとに 2 つの数値の形式で表示します。インターフェイスに関する情報を交換する場合、このユニットはピアに送信するメッセージで最初の数値を使用します。また、ピアから受信されるメッセージでは 2 つ目の数値が予期されます。
details	高可用性ペアを構成するペアのフェールオーバーの詳細を表示します。
Exec	フェールオーバーコマンド実行情報を表示します。
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 [details]	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、アクティブ ユニットの過去のフェールオーバーでの状態変化や、状態変化の理由が表示されます。 フェールオーバー履歴には、失敗の理由と個別の詳細が含まれています。これは、トラブルシューティングに役立ちます。 ピア ユニットからのフェールオーバー履歴を表示するには details キーワードを追加します。これには、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。 履歴情報は、デバイスのリブート時にクリアされます。
interface	フェールオーバーおよびステートフル リンク情報を表示します。
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。

trace [*options*]	（任意）フェールオーバー イベント トレースを表示します。オプションには、フェールオーバー イベント トレースをレベル（1 ～ 5）で表示するオプションが含まれます。 • **critical** ：フェールオーバーの重要なイベントトレースをフィルタ処理（レベル = 1） • **debugging**：フェールオーバーのデバッグトレースをフィルタ処理（デバッグレベル = 5） • **error**：フェールオーバーの内部例外をフィルタ処理（レベル = 2） • **informational**：フェールオーバーの情報トレースをフィルタ処理（レベル = 4） • **warning**：フェールオーバーの警告をフィルタ処理（レベル = 3）
statistics [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync**	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。 • **np-clients**：HA データパスクライアントのパケットの統計情報を表示します。 • **cp-clients**：HA コントロール プレーン クライアントのパケットの統計情報を表示します。 • **bulk-sync**：HA データプレーンクライアント、コントロール プレーン クライアント、または両方の同期時間を表示します。 • **events**：アプリケーション エージェントによって通知されたローカル障害（HA LAN リンクの稼働時間、スーパーバイザのハートビート障害、およびディスクフルの問題）を表示します。 • **all**：interface、np-client、cp-client、および bulk-sync の統合されたフェールオーバー統計情報を表示します。
details	高可用性ペアを構成するペアのフェールオーバーの詳細を表示します。
config-sync	デバイス設定、デバイスステータス、および設定同期の最適化機能に関するチェックサムの詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.1(6)	**details** キーワードが追加されました。
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。
8.2(2)	このコマンドが変更されました。出力には、ファイアウォールインターフェイスおよびフェールオーバー インターフェイスの IPv6 アドレスが含まれます。ステートフル フェールオーバーの統計情報出力には、IPv6 ネイバー探索テーブル（IPv6 ND tbl）の更新についての情報が含まれます。
9.9.2	このコマンドが変更されました。フェールオーバー履歴の出力には、エラー理由の拡張が含まれています。history details キーワードが追加されました。これによりピア ユニットのフェールオーバー履歴が表示されます。
9.16(1)	**details** キーワードが追加されました。
9.18(1)	**config-sync** キーワードが追加されました。
9.20(2)	**statistics all**、**statistics events**、**statistics np-clients**、**statistics cp-clients**、および **statistics bulk-sync** キーワードが追加されました。

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。

IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスには複数の IPv6 アドレスを設定できるため、リンクローカル アドレスのみが表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

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 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：ASA のアップタイムの値（アクティブな ASA がスタンバイの ASA 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。
  - IPv6 ND tbl：IPv6 ネイバー探索テーブル情報。
  - 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 Session：SIP シグナリング セッション情報。
  - Route Session：ルート同期アップデートの LU 統計情報

フェールオーバー IP アドレスを入力しないと、**show failover** コマンドでは IP アドレスが 0.0.0.0 と表示され、インターフェイスのモニタリングが「待機」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 7-1 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 *1:* フェールオーバー インターフェイス状態

状態	説明
標準	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。 フェールオーバー インターフェイスがダウンしたときにも、この状態を確認できます。
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ーされていません。モニター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。
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ーされていません。モニター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ーされていません。モニター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。

状態	説明
不合格	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。

使用上のガイドライン

マルチコンテキストモードでは、セキュリティコンテキストで使用できるのは**show failover**コマンドのみです。オプションのキーワードは入力できません。

例

次に、アクティブ/スタンバイフェールオーバーの**show failover**コマンドの出力例を示します。ASA では、フェールオーバー リンク（folink）と inside インターフェイスに IPv6 アドレスを使用しています。

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 98.1(1)86, Mate 98.1(1)86
Serial Number: Ours JAF1610APKQ, Mate JAF1610ALGM
Last Failover at: 12:52:34 UTC Apr 26 2017
        This host: Primary - Active
                Active time: 87 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.1): Normal (Monitored)
                  Interface outside (192.168.77.1): No Link (Waiting)
                  Interface dmz (192.168.67.1): No Link (Waiting)
                slot 1: empty
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.2): Normal (Waiting)
                  Interface outside (192.168.77.2): No Link (Waiting)
                  Interface dmz (192.168.67.2): No Link (Waiting)
                slot 1: empty
                slot 1: empty
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/4 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         22         0          6          0
        sys cmd         6          0          6          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         14         0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
```

```
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA    0          0          0          0
VPN IKEv2 P2    0          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
SIP Tx  0          0          0          0
SIP Pinhole     0          0          0          0
Route Session   0          0          0          0
Router ID       1          0          0          0
User-Identity   1          0          0          0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
STS Table       0          0          0          0
Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       5       6
Xmit Q:         0       27      86
```

次に、アクティブ/アクティブフェールオーバーの **show failover** コマンドの出力例を示します。この例では、管理コンテキストでのみIPv6アドレスをインターフェイスに割り当てています。

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: folink 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-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): 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-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): 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
        IPv6 ND tbl     22         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 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。

```
ciscoasa(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。

```
ciscoasa(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             12:53:10 UTC Apr 26 2017
====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 7-2 で、 **show failover state** コマンドの出力について説明します。

表 *2 : 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を実行している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。

フィールド	説明
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対して同期されました。 • **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。 • **Interface 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たため、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**
状態	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。

```
ciscoasa(config)# show failover history
==============================================
From State                   To State                     Reason
==============================================
11:59:31 UTC Jan 13 2017
Active Config Applied      Active                       No Active unit found

06:17:51 UTC Jan 15 2017
Active                     Failed                       Interface check
                                                                This Host:3
                                                                  admin: inside
                                                                  ctx-1: ctx1-1
                                                                  ctx-2: ctx2-1
                                                                Other Host:0
03:58:49 UTC Feb 3 2017
Active                     Cold Standby                 Failover state check delayed due
```

```
to  mate failure

03:58:51 UTC Feb 3 2017
Cold Standby               Sync Config               Failover state check delayed due
to  mate failure

03:59:18 UTC Feb 3 2017
Sync Config                Sync File System          Failover state check delayed due
to  mate failure
23:11:39 UTC Jan 13 2017
Cold Standby               Failed                    HA state progression failed as
response not heard from mate

23:19:01 UTC Jan 13 2017
Sync Config                Not Detected              HA state progression failed as
configuration sync timeout expired
 14:26:28 UTC Aug 16 2017
Standby Ready              Just Active               Inspection engine in other unit
has failed due to disk failure

14:26:29 UTC Aug 16 2017
Just Active                Active Drain              Inspection engine in other unit
has failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Drain               Active Applying Config    Inspection engine in other unit
has failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Applying Config     Active Config Applied     Inspection engine in other unit
has failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Config Applied      Active                    Inspection engine in other unit
has failed due to disk failure

18:03:35 UTC Aug 17 2017
Active                     Standby Ready             Other unit wants me Standby

18:03:36 UTC Aug 17 2017
Standby Ready              Failed                    Detect Inspection engine failure
due to disk failure

18:03:37 UTC Aug 17 2017
Failed                     Standby Ready             My Inspection engine is as good
as peer due to disk recovery
```

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。

エラーの理由には、トラブルシューティングに役立つ詳細情報が含まれています。これには、インターフェイス チェック、フェールオーバー状態チェック、状態の進行の失敗、およびサービス モジュールの失敗があります。

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

```
show failover history details
==============================================================================
```

```
From State                 To State                   Reason
================================================================================
09:58:07 UTC Jan 18 2017
Not Detected               Negotiation                No Error
09:58:10 UTC Jan 18 2017
Negotiation                Just Active                No Active unit found
09:58:10 UTC Jan 18 2017
Just Active                Active Drain               No Active unit found
09:58:10 UTC Jan 18 2017
Active Drain               Active Applying Config     No Active unit found
09:58:10 UTC Jan 18 2017
Active Applying Config    Active Config Applied       No Active unit found
09:58:10 UTC Jan 18 2017
Active Config Applied     Active                      No Active unit found
================================================================================
PEER History Collected at 09:58:54 UTC Jan 18 2017
========================PEER-HISTORY============================================
From State                 To State                   Reason
=========================PEER-HISTORY=========================================
09:57:46 UTC Jan 18 2017
Not Detected               Negotiation                No Error
09:58:19 UTC Jan 18 2017
Negotiation                Cold Standby               Detected an Active mate
09:58:21 UTC Jan 18 2017
Cold Standby              Sync Config                 Detected an Active mate
09:58:29 UTC Jan 18 2017
Sync Config              Sync File System             Detected an Active mate
09:58:29 UTC Jan 18 2017
Sync File System         Bulk Sync                    Detected an Active mate
09:58:42 UTC Jan 18 2017
Bulk Sync                Standby Ready                Detected an Active mate
=========================PEER-HISTORY=========================================
```

show failover history details コマンドは、ピアのフェールオーバーの履歴を要求し、ユニットのフェールオーバー履歴とピアの最新のフェールオーバー履歴を出力します。1 秒以内にピアが応答しない場合は、最後に収集されたフェールオーバー履歴情報が表示されます。

表 7-3 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 *3:* フェールオーバーの状態

States	説明
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。
不合格	ユニットは障害状態です。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。

States	説明
Not Detected	ASA はピアの存在を検出できません。このことは、フェールオーバーがイネーブルな状態で ASA が起動されたが、ピアが存在しない、またはピアの電源がオフである場合に発生する可能性があります。
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

次に、**show failover interface** コマンドの出力例を示します。デバイスのフェールオーバー インターフェイスに IPv6 アドレスが設定されています。

```
ciscoasa(config)# show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

次に、**show failover trace** コマンドのフェールオーバー警告出力の例を示します。

```
ciscoasa(config)# show failover trace warning
        Warning:Output can be huge. Displaying in pager mode
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
```

次に、9.18 より前のバージョンに対する **show failover statistics** コマンドのフェールオーバー出力の例を示します。

```
ciscoasa(config)# show failover statistics
        tx:121456
        rx:121306
```

次に、9.18 以降のバージョンに対する **show failover statistics** コマンドのフェールオーバー出力の例を示します。

```
ciscoasa(config)# show failover statistics
        tx:3396
        rx:3296

        Unknown version count for Fover ctl client: 0
        Unknown reason count for peer's switch reason: 0
        fover cd log create failed: 0
```

tx および rx カウンタには、フェールオーバー LAN インターフェイスを介して送受信されるすべての**フェールオーバー制御パケット**が含まれます。

「Unknown version count for Fover ctl client」カウンタは、受信パケットの**フェールオーバー制御パケット**のバージョンが 0 の場合に増加します。

「Unknown reason count for peer's switch reason」カウンタは、**ピアユニットから受信した HA スイッチオーバーの理由がローカルで認識されている理由のリストに含まれていない**場合に増分されます。

fover cd ログファイルハンドルが作成されなかった場合、「fover cd log create failed」は 1 に設定されます。

次に、 **show failover statistics all** コマンドのフェールオーバー出力の例を示します。

```
ciscoasa(config)# show failover statistics all

show failover statistics unit
-----------------------------
Unit Poll frequency 2 seconds, holdtime 10 seconds
Failover unit health statistics set size 10
1 Hold Interval Success: 3 Failure: 0
2 Hold Interval Success: 5 Failure: 0
3 Hold Interval Success: 5 Failure: 0
4 Hold Interval Success: 5 Failure: 0
5 Hold Interval Success: 5 Failure: 0

show failover statistics interface all
--------------------------------------
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 1285 maximum
Health statistics monitored interfaces 3
Failover interface health statistics set size 10
Interface: outside
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0
Interface: inside
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0
Interface: diagnostic
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0

show failover statistics np-clients
-----------------------------------

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error
```

```
HA DP Clients Statistics

TX Statistics
-----------------------------------------------------------------------------------------------------------
Client Name                                          Tx In        Tx Out       BLErr
HIErr        PI
-----------------------------------------------------------------------------------------------------------
SNP HA private client                                  0            0            0
  0            0
Soft NP flow stateful failover                         0            0            0
  0            0
Soft NP SVC stateful failover                          0            0            0
  0            0
SIP inspection engine                                  0            0            0
  0            0
SCTP inspection engine                                 0            0            0
  0            0
Soft NP NLP HA client                                 16           16            0
  0            0
ODNS inspection engine                                 0            0            0
  0            0
DNS BRANCH/SNOOPING module                             0            0            0
  0            0
ARP DP module                                          0            0            0
  0            0
TFW DP module                                          0            0            0
  0            0
SNP HA Heartbeat client                             1130         1130            0
  0            0
ZTNA DP module                                         0            0            0
  0            0
Unknown client                                         0            0            0
  0            0

RX Statistics
-----------------------------------------------------------------------------------------------------------
Client Name                                          Rx In        Rx Out       PSErr
  IPkt         CPkt         PI
-----------------------------------------------------------------------------------------------------------
SNP HA private client                                  0            0            0
    0            0            0
Soft NP flow stateful failover                         0            0            0
    0            0            0
Soft NP SVC stateful failover                          0            0            0
    0            0            0
SIP inspection engine                                  0            0            0
    0            0            0
SCTP inspection engine                                 0            0            0
    0            0            0
Soft NP NLP HA client                                  1            1            0
    0            0            0
ODNS inspection engine                                 0            0            0
    0            0            0
DNS BRANCH/SNOOPING module                             0            0            0
    0            0            0
ARP DP module                                          0            0            0
    0            0            0
TFW DP module                                          0            0            0
    0            0            0
SNP HA Heartbeat client                             1121         1121            0
    0            0            0
ZTNA DP module                                         0            0            0
    0            0            0
```

```
Unknown client                                    0            0            0
    0            0            0

Buffer Failure Statistics
-------------------------------------------------------------------------------------------------------------
Client Name                                     BErr         MDErr        MxBErr
MxBDErr
-------------------------------------------------------------------------------------------------------------
SNP HA private client                            0            0            0
 0
Soft NP flow stateful failover                   0            0            0
 0
Soft NP SVC stateful failover                    0            0            0
 0
SIP inspection engine                            0            0            0
 0
SCTP inspection engine                           0            0            0
 0
Soft NP NLP HA client                            0            0            0
 0
ODNS inspection engine                           0            0            0
 0
DNS BRANCH/SNOOPING module                       0            0            0
 0
ARP DP module                                    0            0            0
 0
TFW DP module                                    0            0            0
 0
SNP HA Heartbeat client                          0            0            0
 0
ZTNA DP module                                   0            0            0
 0
Unknown client                                   0            0            0
 0
-------------------------------------------------------------------------------------------------------------

show failover statistics bulk-sync
-----------------------------------


For session 0, NP Client Bulk Sync stats
=============================================================================================================

 Client Name                          Status              Start Time
End Time         Time Taken
=============================================================================================================

 Soft NP flow stateful failover       Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 Soft NP SVC stateful failover        Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 SCTP inspection engine               Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 DNS BRANCH/SNOOPING module           Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 ARP DP module                        Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 TFW DP module                        Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
 ZTNA DP module                       Done          06:44:50 UTC Feb 10 2023   06:44:50
 UTC Feb 10 2023   00:00:00
=============================================================================================================
```

```
For session 0, CP Client Bulk Sync stats
```

Client Name	Status	Start Time	End Time	Time Taken
HA Internal Control	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Failover Control Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Legacy LU support	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
vpnfo	Done	06:44:50 UTC Feb 10 2023	06:45:00 UTC Feb 10 2023	00:00:10
vpnfo	Done	06:44:50 UTC Feb 10 2023	06:45:00 UTC Feb 10 2023	00:00:10
SIP inspection engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
NetFlow Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
HA Shared License Client	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Route HA engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
CTS	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
CTS SXP Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
IPv6 Route HA engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Service Tag Switching Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
CFG_HIST HA Client	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
SCTP inspection engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
KCD	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
HA CD Proxy Client	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
DHCPv6 HA engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Attribute Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
ODNS inspection engine	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Ruld ID DB Client	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
DNS branch HA CP client	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
DNS_TRUSTED_SOURCE module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
Threat-Detection	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00
ZTNA HA Module	Done	06:44:50 UTC Feb 10 2023	06:44:50 UTC Feb 10 2023	00:00:00

次に、**show failover statistics cp-clients** コマンドの出力例（ゼロ以外の行のみ）を示します。

```
show failover statistics cp-clients
```

```
Abbreviations:
TxIn - Pkt rcvd at HA from client, TxOut - Pkt sent from HA to Interface
BErr - Buffer alloc failure, MDErr - Msg desc alloc failure, AckRcvd - Ack rcvd
ReTx - Retransmit pkts, NoSvc - HA service is down, PIErr - Client is incompatible
EncErr - Error in encrypting pkt, RepCfg - Replace cfg enabled
RxIn - Pkt rcvd from Interface to HA, RxOut - Pkt sent from HA to client
MDErr - Msg desc alloc failure, AckSent - Ack sent, NMsgCb - No Msg callback for client
InVcid - Invalid vcid rcvd, PIErr - Client is incompatible, InvPkt - Invalid pkt rcvd,

HA CP Clients Statistics

TX Statistics
-------------------------------------------------------------------------------------------------------------
Client Name                    TxIn          TxOut       BErr   MDErr  AckRcvd
ReTx   NoSvc  PIErr  EncErr RepCfg
-------------------------------------------------------------------------------------------------------------
Legacy LU Support  478  478 0 0 0  0 0 0 0 0
vpnfo    2  2   0 0 2  0 0 0 0 0
HA CD Proxy Client  17  17  0 0 17       0 0 0 0 0
-------------------------------------------------------------------------------------------------------------
Total Aggressive Ack rcvd      :   0

RX Statistics
-------------------------------------------------------------------------------------------------------------
Client Name                    RxIn          RxOut         MDErr  AckSent       NMsgCb
InVcid PIErr  InvPkt
-------------------------------------------------------------------------------------------------------------
Legacy LU Support  478  478  0 0  0 0 0 0
vpnfo        1960     1960   0 12  0 0 0 0
CTS    1  1      0 1  0 0 0 0
CFG_HIST HA Client  12  12   0 12  0 0 0 0
HA CD Proxy Client  10  10   0 10  0 0 0 0
ZTNA HA Module      1   1    0 1   0 0 0 0
-------------------------------------------------------------------------------------------------------------
Total Aggressive Ack sent        :   0
Total Invalid pkts rcvd          :   0
Total unknown client pkts rcvd   :   0
```

次に、**show failover statistics np-clients** コマンドの出力例（ゼロ以外の行のみ）を示します。

```
show failover statistics np-clients

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error

HA DP Clients Statistics

TX Statistics
-----------------------------------------------------------------------------------------
Client Name                     Tx In          Tx Out       BLErr   HIErr  PI
-----------------------------------------------------------------------------------------
Soft NP flow stateful failover 1420091  1420091 0 0 0
Soft NP NLP HA client    45131    45131   0 0 0
Soft NP NLP HA client current  45129    45129   0 0 0
SNP HA Heartbeat Client  4240     4240    0 0 0
-----------------------------------------------------------------------------------------

RX Statistics
-----------------------------------------------------------------------------------------
Client Name                     Rx In          Rx Out       PSErr   IPkt  CPkt PI

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

```
Soft NP NLP HA client    7943     7943    0 0 0  0
Soft NP NLP HA client current  7943     7943    0 0 0  0
SNP HA Heartbeat client  4185     4185    0 0 0  0
-------------------------------------------------------------------------------------------
Buffer Failure Statistics
-------------------------------------------------------------------------------------------
Client Name                      BErr          MDErr       MxBErr MxBDErr
-------------------------------------------------------------------------------------------
```

Soft NP NLP HA は HA クライアントです。

Soft NP NLP HA Current には、現在のセッションのアプリケーション同期のカウンタが表示されます。

- NP = データプレーン
- Soft NP = データプレーンの内部構造
- NLP = 非 Lina プロセス

次に、フェールオーバーイベントの統計情報を表示する **show failover statistics events** コマンドの出力例を示します。

```
show failover statistics events

Info: Failover Lan interface came UP at 05:01:23 UTC Oct 18 2023
Codes: A -Blade Id, B -Chassis Id C -Re enable failover
=====================================================================
MIO Events Table|                Time              A| B | C|
MIO heartbeat recovered| 05:00:52 UTC Oct 18 2023| 1| 0| true|
MIO heartbeat recovered| 05:04:02 UTC Oct 18 2023| 1| 0|false|
```

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の**failover** コマンドを表示します。

show failover descriptor

フェールオーバーインターフェイス記述子を表示します。インターフェイスごとに2つの数値が表示されます。インターフェイスに関する情報を交換する場合、このユニットはピアに送信するメッセージで最初の数値を使用します。また、ピアから受信されるメッセージでは2つ目の数値が予期されます。トラブルシューティングのために、両方のユニットからの show 出力を収集し、数値が一致するかどうかを確認してください。

show failover descriptor

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2	このコマンドが追加されました。

例

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

```
asa# show failover descriptor
outside send:   20100ffff0001  receive:   20100ffff0002
mgmt    send:   10000ffff0001  receive:   10000ffff0002
inside  send: 20001ffffff0001  receive: 20001ffffff0002
```

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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。このコマンドモードを変更するには、**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）を送信します。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 コマンドを使用すると、指定したデバイスのコマンドモードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

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 回目に入力したとき、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。

```
ciscoasa(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.ciscoasa(config)# failover
exec mate interface GigabitEthernet0/1
ciscoasa(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.ciscoasa(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 failover config-sync

設定同期の最適化機能に関する詳細を表示するには、特権 EXEC モードで **show failover config-sync** コマンドを使用します。

show failover config-sync { **checksum | configuration | status** }

構文の説明

checksum	デバイスのステータスとチェックサムに関する情報を表示します。
configuration	デバイスのフェールオーバー設定とチェックサムに関する情報を表示します。
status	設定同期の最適化ステータスに関する情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.18.(1)	このコマンドが追加されました。

使用上のガイドライン

showfailover config-sync コマンドは、設定同期の最適化機能のステータス、デバイス設定、およびチェックサム情報を表示します。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。

例

次に、アクティブユニットとスタンバイユニットの **showfailoverconfig-synccchecksum** コマンドの出力例を示します。

```
ciscoasa# show failover config-sync checksum
My State: Active
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

```
ciscoasa# show failover config-sync checksum
My State: Standby Ready
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

次に、**showfailoverconfig-syncconfiguration** コマンドの出力例を示します。

```
cicoasa#show failover config-sync configuration
My State: Negotiation
[1]: Cmd_: !
[2]: Cmd_: enable password $sha512$5000$eTI8yiQxuWYEzeypFF6qdw==$HNf7i1tpOugBBnUSIzrlPA==
 pbkdf2
[3]: Cmd_: service-module 0 keepalive-timeout 4
[4]: Cmd_: service-module 0 keepalive-counter 6
[5]: Cmd_: !
[6]: Cmd_: license smart
[7]: Cmd_:  feature tier standard
[8]: Cmd_:  throughput level 10G
[9]: Cmd_: names
[10]: Cmd_: no mac-address auto
[11]: Cmd_: !
[12]: Cmd_: interface GigabitEthernet0/0
[13]: Cmd_:  shutdown
[14]: Cmd_:  no nameif
[15]: Cmd_:  no security-level
[16]: Cmd_:  no ip address
[17]: Cmd_: !
[18]: Cmd_: interface GigabitEthernet0/1
[19]: Cmd_:  shutdown
[20]: Cmd_:  no nameif
[21]: Cmd_:  no security-level
[22]: Cmd_:  no ip address
[23]: Cmd_: !
[24]: Cmd_: interface GigabitEthernet0/2
[25]: Cmd_:  shutdown
[26]: Cmd_:  no nameif
[27]: Cmd_:  no security-level
[28]: Cmd_:  no ip address
[29]: Cmd_: !
[30]: Cmd_: interface GigabitEthernet0/3
[31]: Cmd_:  shutdown
[32]: Cmd_:  no nameif
[33]: Cmd_:  no security-level
[34]: Cmd_:  no ip address
[35]: Cmd_: !
[36]: Cmd_: interface GigabitEthernet0/4
[37]: Cmd_:  shutdown
[38]: Cmd_:  no nameif
[39]: Cmd_:  no security-level
[40]: Cmd_:  no ip address
[41]: Cmd_: !
[42]: Cmd_: interface GigabitEthernet0/5
[43]: Cmd_:  shutdown
[44]: Cmd_:  no nameif
[45]: Cmd_:  no security-level
[46]: Cmd_:  no ip address
[47]: Cmd_: !
[48]: Cmd_: interface GigabitEthernet0/6
[49]: Cmd_:  shutdown
[50]: Cmd_:  no nameif
[51]: Cmd_:  no security-level
[52]: Cmd_:  no ip address
[53]: Cmd_: !
[54]: Cmd_: interface GigabitEthernet0/7
[55]: Cmd_:  shutdown
[56]: Cmd_:  no nameif
[57]: Cmd_:  no security-level
```

```
[58]: Cmd_:  no ip address
[59]: Cmd_: !
[60]: Cmd_: interface GigabitEthernet0/8
[61]: Cmd_:  description LAN/STATE Failover Interface
[62]: Cmd_: !
[63]: Cmd_: interface Management0/0
[64]: Cmd_:  no management-only
[65]: Cmd_:  nameif management
[66]: Cmd_:  security-level 0
[67]: Cmd_:  ip address 192.168.2.63 255.255.255.0 standby 192.168.2.64
[68]: Cmd_: !
[69]: Cmd_: ftp mode passive
[70]: Cmd_: no object-group-search access-control
[71]: Cmd_: pager lines 23
[72]: Cmd_: mtu management 1500
[73]: Cmd_: failover
[74]: Cmd_: failover lan interface fover GigabitEthernet0/8
[75]: Cmd_: failover link fover GigabitEthernet0/8
[76]: Cmd_: failover interface ip fover 10.0.0.63 255.255.255.0 standby 10.0.0.64
[77]: Cmd_: no failover wait-disable
[78]: Cmd_: no monitor-interface service-module
[79]: Cmd_: icmp unreachable rate-limit 1 burst-size 1
[80]: Cmd_: no asdm history enable
[81]: Cmd_: arp timeout 14400
[82]: Cmd_: no arp permit-nonconnected
[83]: Cmd_: arp rate-limit 32768
[84]: Cmd_: route management 0.0.0.0 0.0.0.0 192.168.2.1 1
[85]: Cmd_: timeout xlate 3:00:00
[86]: Cmd_: timeout pat-xlate 0:00:30
[87]: Cmd_: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
[88]: Cmd_: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
[89]: Cmd_: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
[90]: Cmd_: timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
[91]: Cmd_: timeout tcp-proxy-reassembly 0:01:00
[92]: Cmd_: timeout floating-conn 0:00:00
[93]: Cmd_: timeout conn-holddown 0:00:15
[94]: Cmd_: timeout igp stale-route 0:01:10
[95]: Cmd_: user-identity default-domain LOCAL
[96]: Cmd_: aaa authentication ssh console LOCAL
[97]: Cmd_: aaa authentication login-history
[98]: Cmd_: http server enable
[99]: Cmd_: http 0.0.0.0 0.0.0.0 management
[100]: Cmd_: no snmp-server location
[101]: Cmd_: no snmp-server contact
[102]: Cmd_: crypto ipsec security-association pmtu-aging infinite
[103]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA
[104]: Cmd_:  no validation-usage
[105]: Cmd_:  crl configure
[106]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA2
[107]: Cmd_:  no validation-usage
[108]: Cmd_:  crl configure
[109]: Cmd_: crypto ca trustpool policy
[110]: Cmd_:  auto-import
[111]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA
[112]: Cmd_:  certificate ca 0a0142800000014523c844b500000002
[113]: Cmd_:     30820560 30820348 a0030201 0202100a 01428000 00014523 c844b500 00000230

[114]: Cmd_:     0d06092a 864886f7 0d01010b 0500304a 310b3009 06035504 06130255 53311230

[115]: Cmd_:     10060355 040a1309 4964656e 54727573 74312730 25060355 0403131e 4964656e

[116]: Cmd_:     54727573 7420436f 6d6d6572 6369616c 20526f6f 74204341 2031301e 170d3134
```

```
[117]: Cmd_:     30313136 31383132 32335a17 0d333430 31313631 38313232 335a304a 310b3009
[118]: Cmd_:     06035504 06130255 53311230 10060355 040a1309 4964656e 54727573 74312730
[119]: Cmd_:     25060355 0403131e 4964656e 54727573 7420436f 6d6d6572 6369616c 20526f6f
[120]: Cmd_:     74204341 20313082 0222300d 06092a86 4886f70d 01010105 00038202 0f003082
[121]: Cmd_:     020a0282 020100a7 5019de3f 993dd433 46f16f51 6182b2a9 4f8f6789 5d84d953
[122]: Cmd_:     dd0c28d9 d7f0ffae 95437299 f9b55d7c 8ac142e1 315074d1 810d7ccd 9b21ab43
[123]: Cmd_:     e2acad5e 866ef309 8a1f5a32 bda2eb94 f9e85c0a ecff98d2 af71b3b4 539f4e87
[124]: Cmd_:     ef92bcbd ec4f3230 884b175e 57c453c2 f602978d d9622bbf 241f628d dfc3b829
[125]: Cmd_:     4b49783c 93608822 fc99da36 c8c2a2d4 2c540067 356e73bf 0258f0a4 dde5b0a2
[126]: Cmd_:     267acae0 36a51916 f5fdb7ef ae3f40f5 6d5a04fd ce34ca24 dc74231b 5d331312
[127]: Cmd_:     5dc40125 f630dd02 5d9fe0d5 47bdb4eb 1ba1bb49 49d89f5b 02f38ae4 2490e462
[128]: Cmd_:     4f4fc1af 8b0e7417 a8d17288 6a7a0149 ccb44679 c617b1da 981e0759 fa752185
[129]: Cmd_:     65dd9056 cefbaba5 609dc49d f952b08b bd87f98f 2b230a23 763bf733 e1c900f3
[130]: Cmd_:     69f94ba2 e04ebc7e 93398407 f744707e fe075ae5 b1acd118 ccf235e5 494908ca
[131]: Cmd_:     56c93dfb 0f187d8b 3bc113c2 4d8fc94f 0e37e91f a10e6adf 622ecb35 0651792c
[132]: Cmd_:     c82538f4 fa4ba789 5c9cd2e3 0d39864a 747cd559 87c23f4e 0c5c52f4 3df75282
[133]: Cmd_:     f1eaa3ac fd49341a 28f34188 3a13eee8 deff991d 5fbacbe8 1ef2b950 60c031d3
[134]: Cmd_:     73e5efbe a0ed330b 74be2020 c4676cf0 08037a55 807f464e 96a7f41e 3ee1f6d8
[135]: Cmd_:     09e13364 2b63d732 5e9ff9c0 7b0f786f 97bc939a f99c1290 787a8087 15d77274
[136]: Cmd_:     9c557478 b1bae16e 7004ba4f a0ba68c3 7bff31f0 733d3d94 2ab10b41 0ea0fe4d
[137]: Cmd_:     88656b79 33b4d702 03010001 a3423040 300e0603 551d0f01 01ff0404 03020106
[138]: Cmd_:     300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 ed4419c0
[139]: Cmd_:     d3f0068b eea47bbe 42e72654 c88e3676 300d0609 2a864886 f70d0101 0b050003
[140]: Cmd_:     82020100 0dae9032 f6a64b7c 44761961 1e2728cd 5e54ef25 bce30890 f929d7ae
[141]: Cmd_:     6808e194 0058ef2e 2e7e5352 8cb65c07 ea88ba99 8b5094d7 8280df61 090093ad
[142]: Cmd_:     0d14e6ce c1f23794 78b05f9c b3a273b8 8f059338 cd8d3eb0 b8fbc0cf b1f2ec2d
[143]: Cmd_:     2d1bccec aa9ab3aa 60821b2d 3bc3843d 578a961e 9c75b8d3 30cd6008 8390d38e
[144]: Cmd_:     54f14d66 c05d7403 40a3ee85 7ec21f77 9c06e8c1 a7185d52 95edc9dd 259e6dfa
[145]: Cmd_:     a9eda33a 34d0597b daed50f3 35bfedeb 144d31c7 60f4daf1 879ce248 e2c6c537
[146]: Cmd_:     fb0610fa 75596631 4729da76 9a1ce982 aeef9ab9 51f78823 9a699562 3ce55580
[147]: Cmd_:     36d75402 fff1b95d ced4236f d845844a 5b65ef89 0cdd14a7 20cb18a5 25b40df9
[148]: Cmd_:     01f0a2d2 f400c874 8ea12a48 8e65db13 c4e22517 7debbe87 5b172054 51934a53
```

```
[149]: Cmd_:     030bec5d ca33ed62 fd45c72f 5bdc58a0 8039e6fa d7fe1314 a6ed3d94 4a4274d4

[150]: Cmd_:     c3775973 cd8f46be 5538effa e89132ea 97580422 de38c3cc bc6dc933 3a6a0a69

[151]: Cmd_:     3fa0c8ea 728f8c63 8623bd6d 3c969e95 e0494caa a2b92a1b 9c368178 edc3e846

[152]: Cmd_:     e2265944 751ed975 8951cd10 849d6160 cb5df997 224d8e98 e6e37ff6 5bbbaecd

[153]: Cmd_:     ca4a816b 5e0bf351 e1742be9 7e27a7d9 99494ef8 a580db25 0f1c6362 8ac93367

[154]: Cmd_:     6b3c1083 c6addea8 cd168e8d f0073771 9ff2abfc 41f5c18b ec00375d 09e54e80

[155]: Cmd_:     effab15c 3806a51b 4ae1dc38 2d3cdcab 1f901ad5 4a9ceed1 706cccee f457f818

[156]: Cmd_:     ba846e87
[157]: Cmd_:   quit
[158]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA2
[159]: Cmd_:  certificate ca 0509
[160]: Cmd_:     308205b7 3082039f a0030201 02020205 09300d06 092a8648 86f70d01 01050500

[161]: Cmd_:     3045310b 30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164

[162]: Cmd_:     6973204c 696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f

[163]: Cmd_:     6f742043 41203230 1e170d30 36313132 34313832 3730305a 170d3331 31313234

[164]: Cmd_:     31383233 33335a30 45310b30 09060355 04061302 424d3119 30170603 55040a13

[165]: Cmd_:     1051756f 56616469 73204c69 6d697465 64311b30 19060355 04031312 51756f56

[166]: Cmd_:     61646973 20526f6f 74204341 20323082 0222300d 06092a86 4886f70d 01010105

[167]: Cmd_:     00038202 0f003082 020a0282 0201009a 18ca4b94 0d002daf 03298af0 0f81c8ae

[168]: Cmd_:     4c19851d 089fab29 4485f32f 81ad321e 9046bfa3 86261a1e fe7e1c18 3a5c9c60

[169]: Cmd_:     172a3a74 8333307d 615411cb edabe0e6 d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a

[170]: Cmd_:     c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633 e62496f7 3fba5b2b 1c7a35c2

[171]: Cmd_:     d667feab 66508b6d 28602bef d760c3c7 93bc8d36 91f37ff8 db1113c4 9c7776c1

[172]: Cmd_:     aeb7026a 817aa945 83e205e6 b956c194 378f4871 6322ec17 6507958a 4bdf8fc6

[173]: Cmd_:     5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2 e9fe5c98 8cf573af 6bb47ecd

[174]: Cmd_:     d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c 13f1dedd f6c4f889 3fd175f5

[175]: Cmd_:     92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03 fd9cbf5b 16ac92db eafe797c

[176]: Cmd_:     adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53 0c48e60e bdc9b476 0652e611

[177]: Cmd_:     13857263 0304e004 362b2019 02e874a7 1fb6c956 66f07525 dc67c10e 616088b3

[178]: Cmd_:     3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1 b222b653 1cdf351d dca1772a

[179]: Cmd_:     31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f ba2c1515 ea97b3d2 a2b5bef2

[180]: Cmd_:     8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d 82a44c81 e2a1d1ba 675f9507

[181]: Cmd_:     a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51 ce506a08 31f991da 0c8f645c

[182]: Cmd_:     03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc 61dc8b33 77d34432 35096204
```

```
[183]: Cmd_:     921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001 a381b030 81ad300f 0603551d
[184]: Cmd_:     130101ff 04053003 0101ff30 0b060355 1d0f0404 03020106 301d0603 551d0e04
[185]: Cmd_:     1604141a 8462bc48 4c332504 d4eed0f6 03c41946 d1946b30 6e060355 1d230467
[186]: Cmd_:     30658014 1a8462bc 484c3325 04d4eed0 f603c419 46d1946b a149a447 3045310b
[187]: Cmd_:     30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164 6973204c
[188]: Cmd_:     696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f 6f742043
[189]: Cmd_:     41203282 02050930 0d06092a 864886f7 0d010105 05000382 0201003e 0a164d9f
[190]: Cmd_:     065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026 0c0db547 645df8b4 72c946a5
[191]: Cmd_:     03182755 89787d76 ea963480 1720dce7 83f88dfc 07b8da5f 4d2e67b2 84fdd944
[192]: Cmd_:     fc775081 e67cb4c9 0d0b7253 f8760707 4147960c fbe08226 93558cfe 221f6065
[193]: Cmd_:     7c5fe726 b3f73290 9850d437 7155f692 2178f795 79faf82d 26876656 3077a637
[194]: Cmd_:     78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d a256d5a7 2fbc561f cf39c1e2
[195]: Cmd_:     fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a f890d257 a21951a5 2d9741da
[196]: Cmd_:     074fa950 da908d94 46e13ef0 94fd1000 38f53be8 40e1b46e 561a20cc 6f588ded
[197]: Cmd_:     2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f d0f8e4c6 39e90488 3cc3baeb
[198]: Cmd_:     557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1 77680d35 6423acb8 55a103d1
[199]: Cmd_:     4d4219dc f8755956 a3f9a849 79f8af0e b911a07c b76aed34 d0b62662 381a870c
[200]: Cmd_:     f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808 3fe95ef9 3507e4c9 626e577f
[201]: Cmd_:     a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c e1b9825c 5da0c3e9 d848bd19
[202]: Cmd_:     a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7 ef276208 e291195c d2f121dd
[203]: Cmd_:     ba174282 97718153 31a99ff6 7d62bf72 e1a3931d cc8a265a 0938d0ce d70d8016
[204]: Cmd_:     b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0 01506943 9ef4b2ef 6df8ecda
[205]: Cmd_:      f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5 8210eac2 31cd2e
[206]: Cmd_:   quit
[207]: Cmd_: telnet timeout 5
[208]: Cmd_: ssh stack ciscossh
[209]: Cmd_: ssh stricthostkeycheck
[210]: Cmd_: ssh timeout 5
[211]: Cmd_: ssh key-exchange group dh-group14-sha256
[212]: Cmd_: ssh 0.0.0.0 0.0.0.0 management
[213]: Cmd_: console timeout 0
[214]: Cmd_: console serial
[215]: Cmd_: threat-detection basic-threat
[216]: Cmd_: threat-detection statistics access-list
[217]: Cmd_: no threat-detection statistics tcp-intercept
[218]: Cmd_: dynamic-access-policy-record DfltAccessPolicy
[219]: Cmd_: username admin password
$sha512$5000$w9Jv9lDWNVn4XKSG1i0G6Q==$JgmsMmRSYz+ZQX3Ta/bXxA== pbkdf2 privilege 15
[220]: Cmd_: !
[221]: Cmd_: class-map inspection_default
[222]: Cmd_:  match default-inspection-traffic
[223]: Cmd_: !
```

```
[224]: Cmd_: !
[225]: Cmd_: policy-map type inspect dns preset_dns_map
[226]: Cmd_:  parameters
[227]: Cmd_:   message-length maximum client auto
[228]: Cmd_:   message-length maximum 512
[229]: Cmd_:   no tcp-inspection
[230]: Cmd_: policy-map global_policy
[231]: Cmd_:  class inspection_default
[232]: Cmd_:   inspect ip-options
[233]: Cmd_:   inspect netbios
[234]: Cmd_:   inspect rtsp
[235]: Cmd_:   inspect sunrpc
[236]: Cmd_:   inspect tftp
[237]: Cmd_:   inspect dns preset_dns_map
[238]: Cmd_:   inspect ftp
[239]: Cmd_:   inspect h323 h225
[240]: Cmd_:   inspect h323 ras
[241]: Cmd_:   inspect rsh
[242]: Cmd_:   inspect esmtp
[243]: Cmd_:   inspect sqlnet
[244]: Cmd_:   inspect sip
[245]: Cmd_:   inspect skinny
[246]: Cmd_: policy-map type inspect dns migrated_dns_map_2
[247]: Cmd_:  parameters
[248]: Cmd_:   message-length maximum client auto
[249]: Cmd_:   message-length maximum 512
[250]: Cmd_:   no tcp-inspection
[251]: Cmd_: policy-map type inspect dns migrated_dns_map_1
[252]: Cmd_:  parameters
[253]: Cmd_:   message-length maximum client auto
[254]: Cmd_:   message-length maximum 512
[255]: Cmd_:   no tcp-inspection
[256]: Cmd_: !
[257]: Cmd_: service-policy global_policy global
[258]: Cmd_: prompt hostname context
[259]: Cmd_: call-home reporting anonymous prompt 1
[260]: Cmd_: call-home
[261]: Cmd_:  profile License
[262]: Cmd_:   destination address http
https://sch-alpha.cisco.com/its/service/oddce/services/DDCEService
[263]: Cmd_:   destination transport-method http
[264]: Cmd_:  profile CiscoTAC-1
[265]: Cmd_:   no active
[266]: Cmd_:   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
[267]: Cmd_:   destination address email callhome@cisco.com
[268]: Cmd_:   destination transport-method http
[269]: Cmd_:   subscribe-to-alert-group diagnostic
[270]: Cmd_:   subscribe-to-alert-group environment
[271]: Cmd_:   subscribe-to-alert-group inventory periodic monthly
[272]: Cmd_:   subscribe-to-alert-group configuration periodic monthly
[273]: Cmd_:   subscribe-to-alert-group telemetry periodic daily
My State: Negotiation
Config content_size: 11323
Config Hash: 9d653d6fb48739651f5467a1aebea31c
```

次に、デバイスで設定同期の最適化機能が有効になっている場合の **showfailoverconfig-syncstatus** コマンドの出力例を示します。

```
ciscoasa# show failover config-sync status
Config Sync Optimization is enable
```

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関する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。
filename	ファイル名を指定します。
information	パートナー アプリケーション パッケージ ファイルなど、特定のファイルについての情報を表示します。
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	パートナー アプリケーション パッケージ ファイルについての情報を表示する機能が追加されました。
9.7(1)	**show file descriptor** コマンドは、システム コンテキスト モードで open ファイル記述子からだけ出力をプリントするように更新されました。

使用上のガイドライン

マルチコンテキストモードのシステムコンテキストで使用する場合、**show file descriptors** コマンドはすべてのコンテキストにわたって、開いている場合のファイルの記述子の詳細を表示します。コンテキストに open ファイル記述子がある場合、CLI がシステム コンテキストで実行されていれば、その特定のコンテキストの詳細のみが表示されます。システムは、「no file

descriptors」のコンテキストのすべての名前は出力しません。open ファイル記述子があるコンテキストのみを表示します。

例

次に、**show firewall** コマンドの出力例を示します。

Single context with no open file

```
ciscoasa(config)# show file descriptors
No open file descriptors
ciscoasa(config)#
```

Single context with open files

```
ciscoasa(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0302  139  disk0:/test1.txt
ciscoasa(config)#
```

Multicontext with no open files in the System context

```
ciscoasa# show file descriptors
ciscoasa#
```

Multicontext with open files in the System context

```
ST-Campus-spyc/stby(config)# show file descriptors
Context: CTX1
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX3
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX5
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
```

Multicontext with no open files in the User context

```
ST-Campus-spyc/stby/CTX1(config)# changeto context CTX2
ST-Campus-spyc/act/CTX2(config)# show file descriptors
No open file descriptors
ST-Campus-spyc/act/CTX2(config)#
```

Multicontext with open files in the User context

```
ST-Campus-spyc/stby(config)# changeto con CTX1
ST-Campus-spyc/stby/CTX1(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
ST-Campus-spyc/stby/CTX1(config)#
ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

次に、**show file info** コマンドの出力例を示します。

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

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 fips

FIPS のステータスを表示するには、特権 EXEC モードで **show fips** コマンドを使用します。

show fips

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが追加されました。

使用上のガイドライン

show running-configuration fips コマンドでは、FIPS が有効になったときにのみステータスが表示されていました。**show fips** コマンドは、実際の動作状態を把握するために導入されました。したがって、このコマンドでは、ユーザーが無効または有効状態になっている FIPS を有効または無効にするときに、FIPS ステータスが表示されます。また、このコマンドで、アクションを有効化または無効化した後でデバイスを再起動するためのステータスも表示されます。

例

次に、**show fips** コマンドの出力例を示します。

FIPS が無効になっていて、ユーザーが **fips enable** を実行してこれを有効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently disabled and will be enabled after reboot
```

ASA のリブート後、

```
ciscoasa# show fips
FIPS is currently enabled
```

FIPS が有効になっていて、ユーザーが **no fips enable**を実行してこれを無効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently enabled and will be disabled after reboot
```

ASA のリブート後、

```
ciscoasa# show fips
FIPS is currently disabled
```

FIPS が無効になっていて、ユーザーが **no fips enable** を実行してこれを無効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently disabled
```

FIPS が有効になっていて、ユーザーが **fips enable** を実行してこれを有効にすると、次のようになります。

```
ciscoasa# show fips
FIPS is currently enabled
```

関連コマンド

コマンド	説明
fips enable	ASA で FIPS を有効にします。
show running-configuration fips	fipsの現在の実行コンフィギュレーションと動作コンフィギュレーションを表示します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show firewall** コマンドの出力例を示します。

```
ciscoasa# 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: all | controller | filesys

（注） ASA では、**flash** キーワードにエイリアス **disk0** が使用されます。

構文の説明

all	すべてのフラッシュの情報を表示します。
controller	ファイル システム コントローラの情報を表示します。
filesys	ファイル システムの情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show flash:** コマンドの出力例を示します。

```
ciscoasa# 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 flow-export counters

NetFlow データに関連付けられているランタイムカウンタを表示するには、特権 EXEC モードで **show flow-export counters** コマンドを使用します。

show flow-export counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
9.0(1)	送信元ポート割り当ての失敗に対する新しいエラーカウンタが追加されました。

使用上のガイドライン

ランタイム カウンタには、統計データおよびエラー データが含まれます。

例

次に、NetFlow データに関連付けられているランタイムカウンタを表示する **show flow-export counters** コマンドの出力例を示します。

```
ciscoasa# show flow-export counters
destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                      1000
 Errors:
  block allocation failure             0
  invalid interface                    0
  template send failure                0
  no route to collector                0
  source port allocation               0
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。

show flow-offload

フローオフロードについての情報を表示するには、特権 EXEC モードで **show flow-offload** コマンドを使用します。

show flow-offload { **info** [**detail**] **| cpu | flow** [**count | detail**] **| statistics** }

構文の説明

info [**detail**]	オフロード エンジンに関する基本情報を表示します。ポートの使用状況の要約などの追加情報を取得するには、**detail** キーワードを追加します。
cpu	オフロード コアの負荷のパーセンテージを表示します。
flow [**count** | **detail**]	オフロードされているアクティブなフローに関する情報を表示します。オプションで次のキーワードを追加できます。 • **count** ：オフロードされているアクティブなフローと作成済みのオフロードされたフローの数を表示します。 • **detail** ：オフロードされているアクティブなフローとそれらの書き換えルールとデータを表示します。
statistics	オフロードされたフローのパケット統計情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(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

フローオフロードが有効な場合は、このコマンドを使用して、サービスとオフロードされたフローに関する情報を表示できます。

例

show flow-offload flow コマンドの出力例を次に示します。オフロードされたフローは、送信元と宛先の IP アドレス、ポート、およびプロトコルをハッシュすることによって計算されるインデックス番号によって識別されます。システムが現在アクティブなオフロードされたフローと同じインデックスを持つフローをオフロードしようとすると、衝突が発生します。この場合、新しいフローはオフロードされませんが、最初のフローはオフロードされたままになります。

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
 84040, bytes 127404640
```

次に、**show flow-offload statistics** コマンドの出力例を示します。出力には、送信（Tx）パケット数、受信（Rx）パケット数、ドロップされたパケット数、および使用された仮想 NIC（VNIC）の統計情報が示されます。

```
ciscoasa# show offload-engine statistics

Packet stats of port : 0
        Tx Packet count                 :        785807566
        Rx Packet count                 :        785807566
        Dropped Packet count            :                0
        VNIC transmitted packet         :        785807566
        VNIC transmitted bytes          :     103726598712
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
 Packet stats of port : 1
        Tx Packet count                 :                0
        Rx Packet count                 :                0
        Dropped Packet count            :                0
        VNIC transmitted packet         :                0
        VNIC transmitted bytes          :                0
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

詳細情報の例を次に示します。

```
ciscoasa(config)# show flow-offload info detail

Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload         : Enabled
Offload App                  : Running
Offload allocated cores      : S0[ 2]
Offload Nic                  : 9
Max PKT burst                : 32
Port-0 details :
        FQ queue number      :           1440
        Keep alive counter   :         101584
flow table refresh count     : 186 [58]
HW flow table refresh count  : Port-0[58, 58, 58, 58]
Refresh count synched        : 3 times [3/0]
Flow table status Port-0     : Good
```

出力の下部にある更新回数情報は、ソフトウェア（ASA）およびハードウェアに保持されているフローテーブルのステータスを示します。「更新回数」はフローテーブルが無効化された回数です。無効化の原因としては、ソフトウェアからハードウェアへのルート変更（追加/削除）、MAC アドレスの変更など、複数のイベントが考えられます。

- フローテーブル更新回数は、フローテーブルを無効化する必要があった回数です。この値は、ASA ソフトウェアで維持されます。
- ハードウェアフローテーブル更新回数は、ハードウェアフローテーブルが無効化された回数です。この値は、ハードウェアで維持されます。
- 同期された更新回数は、「フローテーブル更新回数」がソフトウェアからハードウェアに明示的に同期された回数です。これは、ソフトウェアとハードウェア間に不一致があるたびに発生します。通常、「フローテーブル更新回数」と「HW フローテーブル更新回数」は同期されるため、明示的に値を同期する必要はありません。通常、「同期された更新回数」パラメータはゼロです。
- 「フローテーブルステータス」は、Good または Bad です。Good は、「フローテーブル更新回数」と「HW フローテーブル更新回数」が同期していることを示します。Bad は、明示的に同期を試みた後でも、不一致であることを示します。これは、CRUZ ファームウェアがスタックしているか、ASA ソフトウェアからの更新要求に応答しないなど、まれな状態で発生する可能性があります。

関連コマンド

コマンド	説明
clear flow-offload	オフロード統計情報またはフローをクリアします。
flow-offload	フロー オフロードを有効にします。
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。

show flow-offload-ipsec

IPsec フローオフロードに関する情報を表示するには、特権 EXEC モードで **show flow-offload-ipsec** コマンドを使用します。

show flow-offload-ipsec { **info** | **option-table** | **statistics** }

構文の説明

info	IPsec フローオフロードの現在の設定状態に関する情報を表示します。
option-table	IPsec フローオフロードで使用される Content Addressable Memory（CAM）のテーブル情報を表示します。この情報はデバッグにのみ使用され、エンドユーザーにとっては意味はありません。
statistics	オフロードされたフローの Content Addressable Memory（CAM）の統計を表示します。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.18(1)	このコマンドが導入されました。

例

次に、IPsec フローオフロードの現在の設定状態を表示する例を示します。

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

次に、統計を表示する例を示します。

```
ciscoasa# show flow-offload-ipsec statistics

        Packet stats of Pipe 0
        ----------------------
```

```
        Rx Packet count                                 :               0
        Tx Packet count                                 :               0
        Error Packet count                              :               0
        Drop Packet count                               :               0

        CAM stats of Pipe 0
        -----------------------
        Option ID Table CAM Hit Count                   :              38
        Option ID Table CAM Miss Count                  :             154
        Tunnel Table CAM Hit Count                      :               0
        Tunnel Table CAM Miss Count                     :               0
        6-Tuple CAM Hit Count                           :               0
        6-Tuple CAM Miss Count                          :              38
```

次に、オプションテーブルを表示する例を示します。

```
ciscoasa# show flow-offload-ipsec option-table
        instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0
```

関連コマンド

コマンド	説明
clear flow-offload-ipsec	IPsec フローオフロードの統計をクリアします。
flow-offload-ipsec	IPsec フローオフロードを設定します。

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）ASA のインターフェイスを指定します。

コマンド 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。

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

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。
9.15(1)	**show fragment** コマンドの出力が拡張され、IP フラグメント関連のドロップカウンタとエラーカウンタが含まれるようになりました。

例

次に、IP フラグメント再構成モジュールの動作データを表示する例を示します。

```
ciscoasa# show fragment
Interface: inside
    Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats: Queue: 0, Full assembly: 12
    Drops: Size overflow: 0, Timeout: 0,
           Chain overflow: 0, Fragment queue threshold exceeded: 0,
           Small fragments: 0, Invalid IP len: 0,
           Reassembly overlap: 26595, Fraghead alloc failed: 0,
           SGT mismatch: 0, Block alloc failed: 0,
           Invalid IPV6 header: 0
```

それぞれの説明は次のとおりです。

- [Size]：デフォルトとして設定した任意のポイントで、フラグメントデータベース（インターフェイスごと）に存在できるブロックの最大数。
- チェーン（Chain）：完全な IP パケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは 24 です。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するのを待機する最大秒数を指定します。デフォルトは 5 秒です。
- リアセンブル（Reassembly）：仮想（virtual）または完全（full）。デフォルトは virtual です。IP フラグメントが ASA で終了する場合やアプリケーション レベルでインスペクションを必要とする場合には、完全（物理的）にリアセンブルされます。必要に応じて、完全（物理的）にリアセンブルされたパケットは、出力インターフェイスで再度フラグメント化できます。
- ランタイム統計（Runtime stats）：キュー。リアセンブルデータベースで現在リアセンブルを待機しているフラグメントの数。
- ランタイム統計（Runtime stats）：フルアセンブリ。完全にリアセンブリされた IP パケットの数。
- [Size Overflow]：任意の時点でフラグメントデータベースに存在できるブロックの最大数に達しました。オーバーフローカウンタでは、フラグメントデータベースのデフォルトサイズに達したことによるドロップ数が測定されます。このカウンタには、キューサイズ（最大 DB サイズの 2/3）が原因でドロップされたフラグメントの数は含まれません。
- [Timeout]：再構築が完了する前にフラグメントチェーンがタイムアウトしました。
- [Chain limit]：個々のフラグメントチェーンの制限に達しました。
- [Fragment queue threshold exceeded]：フラグメントデータベースのしきい値（インターフェイスあたりのキューサイズの 2/3）を超過しています。
- [Small fragments]：フラグメントオフセットが 0 より大きく 16 より小さい場合。
- [Invalid packet len]：無効な IP パケット長（例、パケット長 > 65535）。
- [Reassembly overlap]：重複またはオーバーラップしているフラグメントが検出されました。
- [Fraghead alloc failed]：フラグメントヘッドの割り当てに失敗しました。Fraghead には、IP パケットのすべてのフラグメントのチェーンが維持されます。
- [SGT mismatch]：同じ IP パケットのフラグメント間で SGT 値が一致しませんでした。
- [Block alloc failed]：完全な再構築の割り当てに失敗しました。
- [Invalid IPV6 header]：完全な再構築中に無効な IPV6 ヘッダーが検出されました。

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。
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 fxos mode

アプライアンスモードまたはプラットフォームモードの Firepower 2100 を表示するには、特権 EXEC モードで **show fxos mode** コマンドを使用します。

show fxos mode

（注） このコマンドは Firepower 2100 のみでサポートされています。

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。

コマンド デフォルト

デフォルトでは、モードはアプライアンスモードに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 2100 は、FXOS と呼ばれる基盤となるオペレーティングシステムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Secure Firewall シャーシマネージャ（旧 Firepower Chassis Manager） Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

現在のモードを表示するには、**show fxos mode** を使用します。

例

次に、**show fxos mode** コマンドの出力例を示します。

```
ciscoasa# show fxos mode
Mode is currently set to appliance
```

関連コマンド

コマンド	説明
connect fxos	FXOS CLI に接続します。
fxos mode appliance	モードをアプライアンスモードに設定します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show gc** コマンドの出力例を示します。

```
ciscoasa# 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

ASA 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h225 コマンドは、ASA 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。

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。多数のセッションレコードが存在するときに **pager** コマンドが設定されていないと、**show** の出力が完了する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。

```
ciscoasa# 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 ASA 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ものの、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
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 ASA 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	ASA 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 ASA 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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 ASA 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 チャネルで H.225 メッセージの一部として交換された場合です。

例

次に、**show h245** コマンドの出力例を示します。

```
ciscoasa# 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
```

ASA 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。このヘッダーで、こ

の 4 バイトのヘッダーを含むメッセージの長さがわかります）。外部のホストのエンドポイントは、172.30.254.203 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。

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、論理チャネル番号（LCN）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
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 ASA 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	ASA 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

H.323 接続の情報を表示するには、特権 EXEC モードで show **h323** コマンドを使用します。

show h323 { **ras | gup** }

構文の説明

ras	ASA 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 セッションを表示します。
gup	H323 ゲートウェイ アップデート プロトコル接続に関する情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h323 ras コマンドは、ASA 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。

例

次に、**show h323 ras** コマンドの出力例を示します。

```
ciscoasa# show h323 ras
ciscoasa#
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

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
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。

コマンド	説明
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 ASA 間で確立された H.245 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 hardware-bypass

ISA 3000上の現在のハードウェアバイパスのステータスを表示するには、特権 EXEC モードで **show hardware-bypass** コマンドを使用します。

show hardware-bypass

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

例

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

```
ciscoasa# show hardware-bypass

                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

関連コマンド

コマンド	説明
hardware-bypass	ISA 3000 デバイスでハードウェア バイパス モードを設定します。

show history

以前入力したコマンドを表示するには、ユーザー 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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

次に、ユーザー EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa> show history
show history
help
show history
```

次に、特権 EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa
#
 show history
show history
help
show history
enable
show history
```

次に、グローバル コンフィギュレーション モードで **show history** コマンドを使用する例を示します。

```
ciscoasa(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 hostname

ホスト名を表示するには、特権 EXEC モードで **show hostname** コマンドを使用します。

show hostname [**fqdn**]

構文の説明

fqdn	完全修飾ドメイン名を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	コマンドが追加されました。

使用上のガイドライン

hostname コマンドを使用してホスト名を設定し、**domain-name** コマンドを使用してドメインを設定します。

例

次に、show hostname fqdn コマンドの出力例を示します。

```
ciscoasa# show hostname fqdn
asa1.cisco.com
```

関連コマンド

コマンド	説明
hostname	ASA のホスト名を設定します。
domain-name	ASA のドメイン名を設定します。

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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはすでに存在していました。

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。

```
ciscoasa# 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	ASA インターフェイスが終端となる 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。出力の説明については、「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。

```
ciscoasa# 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 7-4 に、各フィールドの説明を示します。

表 *4 : 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

ASA 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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、直接接続されたすべての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。

```
ciscoasa# 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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関する情報を表示します。

例

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

```
ciscoasa# 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	ASA 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# 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。

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

show import webvpn

ASA または セキュアクライアント をカスタマイズおよびローカライズする、フラッシュメモリ内のファイル、カスタマイゼーション オブジェクト、変換表、またはプラグインを一覧表示するには、特権 EXEC モードで **show import webvpn** コマンドを使用します。

show import webvpn { **AnyConnect-customization | customization | mst-translation | plug-in | translation-table | url-list | webcontent** } [**detailed | xml-output**]

構文の説明

AnyConnect-customization	セキュアクライアントGUIをカスタマイズする、ASAフラッシュメモリ内のリソースファイル、実行ファイルおよびMS変換を表示します。
customization	クライアントレス VPN ポータルをカスタマイズする、ASA フラッシュメモリ内の XML カスタマイゼーション オブジェクトを表示します（ファイル名は base64 デコード済み）。
mst-translation	セキュアクライアントインストーラプログラムを変換する、ASAフラッシュメモリ内の MS 変換を表示します。
plug-in	ASA フラッシュメモリ内のプラグインモジュールを表示します（SSH、VNC、およびRDPなどのサードパーティのJavaベースのクライアント アプリケーション）。
translation-table	クライアントレスポータル、Secure Desktopおよびプラグインによって表示されるユーザーメッセージの言語を変換する、ASA フラッシュメモリ内の変換テーブルを表示します。
url-list	クライアントレスポータルによって使用される、ASA フラッシュメモリ内の URL の一覧を表示します（ファイル名は base64 デコード済み）。
webcontent	クライアントレスポータル、クライアントレス アプリケーションおよびプラグインによって、エンドユーザーに表示されるオンラインヘルプに使用される、ASA フラッシュメモリ内のコンテンツを表示します。
detailed	フラッシュ メモリ内のファイルおよびハッシュのパスを表示します。
xml-output	ファイルの XML を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	AnyConnect-customization キーワードが追加されました。

使用上のガイドライン

show import webvpn コマンドを使用すると、クライアントレス SSL VPN ユーザー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、ASA 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。

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。

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#
ciscoasa#  show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization

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

Template
```

```
No bookmarks are currently defined
ciscoasa#
ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn all	ASA 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* | **vni** *id* [**summary**]] [**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と、SSM の内部インターフェイスが ASA 5500 にインストールされている場合は、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、ユーザー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）インターフェイス ID（**gigabit ethernet 0/1** など）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。
redundant *number*	（任意）冗長インターフェイス ID（**redundant 1** など）を指定します。
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。
summary	（オプション）VNI インターフェイスの場合は、VNI インターフェイスのパラメータのみを表示します。
サブインターフェイス	（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*	（オプション）Firepower 1010、ASA 5505、または ASASM の場合に、VLAN インターフェイスを指定します。
vni *id*	（オプション）VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。

コマンド 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。

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

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)	4GE SSM インターフェイスのサポートが追加されました。
7.2(1)	スイッチ インターフェイスのサポートが追加されました。
8.0(2)	冗長インターフェイス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。
8.2(1)	No buffer の数値が、ブロック割り当てからの失敗の数を示すように変更されました。
8.6(1)	ASA 5512-X ～ ASA 5555-X の共有管理インターフェイス、およびソフトウェア モジュールのコントロールプレーン インターフェイスのサポートが追加されました。管理インターフェイスは **show interface detail** コマンドを使用して Internal-Data0/1 として表示され、コントロール プレーン インターフェイスは Internal-Control0/0 として表示されます。
9.4(1)	**vni** インターフェイスタイプが追加されました。
9.5(1)	クラスタリング サイト固有の MAC アドレスが出力に追加されました。
9.10(1)	Firepower 2100/4100/9300 の場合、コマンドの出力は、インターフェイスのスーパーバイザの関連付けステータスを表示するために強化されています。
9.13(1)	アプライアンスモードでの Firepower 1000 シリーズおよび Firepower 2100 のサポートが追加されました。

リリース	変更内容
9.17(1)	VNI インターフェイスについて、シングルアームプロキシが有効になっているかどうかを示します。Cisco Secure Firewall 3100 の場合は FEC モードを示し、**detail** オプションの場合はキューの出力インターフェイスを示します。

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、ASA 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、ASA 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、ASA 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） ハードウェアカウントとトラフィック統計カウントでは、送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。一方トラフィック統計には、レイヤ 3 パケット 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よって異なります。たとえば、ファスト イーサネット カードの場合は、イーサネット ヘッダーが含まれるため、レイヤ 2 カウントのほうがトラフィック カウントより 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。

出力の説明については、「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。

```
ciscoasa# 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
```

次の出力は、使用している場合のサイト MAC アドレスの使用状況を示しています。

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

表 7-5 に、各フィールドの説明を示します。

表 *5 : show interface* の各フィールド

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、ASA 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 識別子	サブインターフェイスの場合、VLAN ID。

フィールド	説明
ハードウェア	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
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。

フィールド	説明
Site Specific MAC address	クラスタリングの場合に、使用中のサイト固有の MAC アドレスを表示します。
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 サーバー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。
サブネット マスク	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	ブロック割り当てからの失敗の数。
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。
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、ASA 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。

フィールド	説明
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	ASA のデータ処理能力を入力レートが超えたため、ASA 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。
中断	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。冗長インターフェイス コンフィギュレーションのスタンバイインターフェイスでは、このインターフェイスに名前（**nameif** コマンド）が設定されていないため、カウンタが増加する可能性があります。
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	ASA 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、ASA 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）。

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 番めのホストが 1 番め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、ASA はパケットの送信を部分的に完了しています。ASA 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のみ）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）。
ハードウェア	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）。
ハードウェア	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。

フィールド	説明
input queue (blocks free curr/low)	curr/low エントリは、インターフェイスの受信（入力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メインCPUによって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。
output queue (blocks free curr/low)	curr/low エントリは、インターフェイスの送信（出力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メインCPUによって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。
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、高速セキュリティパス（ASP）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。
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。

例

次に、スイッチポートを含む ASA 5505 上での **show interface** コマンドの出力例を示します。

```
ciscoasa# 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 7 : show interface detail の各フィールド に、Firepower 1010 または ASA 5505 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 7-6 を参照してください。

表 *6 :* スイッチ インターフェイスについての *show interface* の各フィールド

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ー設定のスイッチ 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。 • ASA 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。
switch egress policy drops	現在使用されていません。

Cisco Secure Firewall 3100 に対する **show interface** コマンドの次の出力例は、FEC モードを auto（cl74-fc を使用）として示しています。

```
ciscoasa(config-if)# sh int eth1/5
Interface Ethernet1/5 "", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
   Full-Duplex(fullDuplex), 25000 Mbps(25gbps)
   Available but not configured via nameif
   MAC address fc58.9a06.9112, MTU not set
   IP address unassigned
   FEC mode is auto(cl74-fc)
   13 packets input, 2165 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 pause input, 0 resume input
   0 packets output, 0 bytes, 0 underruns
   0 pause output, 0 resume output
   0 output errors, 0 collisions, 0 interface resets
```

```
   0 late collisions, 0 deferred
   0 input reset drops, 0 output reset drops
```

例

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。

```
ciscoasa# 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 7 : show interface detail の各フィールドに、 **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 7 : show interface detail の各フィールドを参照してください。

表 *7: 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）ASA 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。
インターフェイスの状態	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、ASA 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。
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。

次に、ASA 5512-X ～ ASA 5555-X 上の **show interface detail** コマンドの出力例を示します。この例では、ASA とソフトウェアモジュールの両方の管理 0/0 インターフェイス（「Internal-Data0/1」として表示）の統計情報を組み合わせて示しています。出力には、Internal-Control0/0 インターフェイスも示されています。これは、ソフトウェアモジュールと ASA 間の制御トラフィックに使用されています。

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, 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 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        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
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, 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 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        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
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

Cisco Secure Firewall 3100 に対する **show interface detail** については、キューの出力インターフェースを示している次の出力を参照してください。

```
ciscoasa# show interface detail
Interface Internal Data0/1 "", is up, line protocol is up
```

```
   Hardware is , BW 500000 Mbps, DLY 1000 usec
      (Full duplex), (50000 Mbps)
      [...]
         TX[64]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
         TX[65]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
```

show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 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
```

show interface vni 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

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。

コマンド	説明
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）インターフェイス ID（ **gigabit ethernet0/1** など）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。
サブインターフェイス	（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。

コマンド デフォルト

インターフェイスを指定しない場合、ASA 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 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。
9.10(1)	Firepower 2100/4100/9300 デバイスのスーパバイザ アソシエーション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。

出力の説明については、「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。

```
ciscoasa# 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   admin  down            down
    GigabitEthernet0/2          10.1.1.50       YES manual  admin down            down
    GigabitEthernet0/3          192.168.2.6     YES DHCP    admin down            down
    Management0/0               209.165.201.3   YES CONFIG  up
The following is sample output from the show ip brief
command on ASA with FXOS:
ciscoasa# sh int ip br
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/0           unassigned      YES           unset  up          up
Vlan10                     172.18.249.190  YES           CONFIG up          up
Vlan80                     80.1.1.1        YES           manual up          up
Vlan300                    14.30.1.1       YES           CONFIG up          up
....
Ethernet1/1                unassigned      YES           unset  up          up
Ethernet1/2                unassigned      YES           unset  down        down
Ethernet1/3                unassigned      unassociated  unset  admin down  down
Ethernet1/4                unassigned      unassociated  unset  admin down  down
Ethernet1/5                unassigned      YES           unset  up          up
Ethernet1/6                unassigned      unassociated  unset  down        down
Ethernet1/7                unassigned      unassociated  unset  down        down
Ethernet1/8                unassigned      unassociated  unset  up          up
Internal-Data1/1           169.254.1.1     YES           unset  up          up
Management1/1              unassigned      YES           unset  up          up
BVI50                      50.1.1.3        YES           CONFIG up          up
Port-channel3              unassigned      YES           unset  down        down
Port-channel8              8.0.0.1         YES           manual up          up
```

例

表 7 : show interface detail の各フィールド に、各フィールドの説明を示します。

表 *8 : show interface ip brief* の各フィールド

フィールド	説明
インターフェイス（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と、AIP SSM の内部インターフェイスが ASA にインストールされている場合は、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、ユーザー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。

フィールド	説明
OK?	インターフェイスがスーパーバイザに関連付けられていない場合、この列には「unassociated」と表示されます。インターフェイスがスーパーバイザに関連付けられている場合は「YES」と表示されます。この状態は、Firepower 2100/4100/9300 インターフェイスとデバイスにのみ適用されます。 FXOS ベースの ASA デバイスの場合は、インターフェイスがポートチャネルに追加されるとこの列に「unassociated」と表示されます。 その他のデバイスでは、この列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 サーバーから受信しました。
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。 • admin 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。

コマンド	説明
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

製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）が割り当てられているネットワーク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、ユーザー EXEC モードで **show inventory** コマンドを使用します。

show inventory *mod_id*

構文の説明

mod_id （オプション）モジュール ID またはスロット番号（0 ～ 3）を指定します。

コマンド デフォルト

項目のインベントリを表示するスロットを指定しない場合は、すべてのモジュール（電源モジュールを含む）のインベントリ情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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。
8.4(2)	SSP の出力が追加されました。さらに、デュアル SSP インストールのサポートが追加されました。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X および 5555-X（シャーシ、冗長電源、I/O 拡張カード）の出力が追加されました。
9.1(1)	ASA CX モジュールの出力が追加されました。

使用上のガイドライン

show inventory コマンドは、各シスコ製品に関するンベントリ情報を UDI 形式で取得および表示します。UDI形式とは、製品ID（PID）、バージョンID（VID）、およびシリアル番号（SN）という 3 つの異なるデータ要素の組み合わせです。

PID は製品を発注するための名前で、従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用する ID です。

VIDは製品のバージョンです。製品が変更されると、VIDは、製品の変更通知を管理する業界ガイドラインである Telcordia GR-209-CORE から定めた厳格なプロセスに従って増分されます。

SN はベンダー固有の製品の通し番号です。それぞれの製品には工場で割り当てた独自のシリアル番号があり、現場では変更できません。シリアル番号は、製品の個々の固有のインスタンスを識別するための手段です。シリアル番号は、デバイスのさまざまなコンポーネントに応じてその長さが異なる場合があります。

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。

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。

（注） 2 つの SSP が同じシャーシに取り付けられている場合は、モジュールの番号がシャーシ内でのモジュールの物理的な場所を示します。スロット 0 に取り付けられた SSP が、常にシャーシマスターとなります。センサーは、SSPが関連付けられている場合にのみ、出力に表示されます。出力内の用語 *module* は、物理スロットと同等です。SSP 自体の説明においては、物理スロット 0 に取り付けられている場合には出力に module: 0、それ以外の場合は module: 1 が含まれます。ターゲット SSP がシャーシマスターである場合、**show inventory** コマンドの出力には電源や冷却ファンが含まれます。それ以外の場合、これらのコンポーネントは省略されます。

ASA 5500-X シリーズのハードウェア上の制限により、シリアル番号が表示されない場合があります。これらのモデルの PCI-E I/O（NIC）オプション カードの UDI 表示では、カード タイプは 2 つのみですが、出力はシャーシ タイプに応じて 6 通りになります。これは、指定されたシャーシに応じて異なる PCI-E ブラケット アセンブリが使用されるためです。次に、各 PCI-E I/O カード アセンブリについて予想される出力を示します。たとえば、Silicom SFP NIC カードが検出された場合、UDI 表示はこのカードが取り付けられているデバイスによって決定されます。VID および S/N の値は N/A です。これは、これらの値が電子的に格納されていないためです。

ASA 5512-X または 5515-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X または 5515-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

例

次に、キーワードや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。この出力例は、ASA に取り付けられている、PID が割り当てられている各シスコエンティティのリストを示しています（ASA CX モジュール用に使用されているストレージデバイスを含む）。

```
ciscoasa> show inventory

Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555           , VID: V01     , SN: FGL170441BU
Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC        , VID: N/A     , SN: 2CS1AX
Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A               , VID: N/A     , SN: MXA174201RR
```

次に、デュアル SSP インストールのシャーシマスター上の **show inventory** コマンドの出力例を示します。

```
ciscoasa> show inventory

Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40    , VID: V01     , SN: JAF1436ACLJ
Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V01     , SN: 123456789AB
Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN       , VID: V01     , SN: POG1434000G
Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V01     , SN: POG1434002K
```

このコマンドは取り外し可能なモジュールのみを表示します。したがって、ASA で **show interface brief** を実行すると、EPM のすべての SFP インターフェイスが表示されますが、ASA で **show inventory** コマンドを実行すると、SFP が接続されているインターフェイスのデータのみが表示されます。次に、接続されている SFP インターフェイスでの **show inventory** コマンドの出力例を示します。

```
ciscoasa> show inventory
```

```
Name: "Ethernet 1/13", DESCR: "h10g-acu1m"
PID: SFP-10G-AOC1M, VID: , SN: A4Z1942K0UC-B
```

表 7-9 に、この出力で表示されるフィールドについて説明します。

表 *9 : show inventory* のフィールドの説明

フィールド	説明
名前	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、コンソール、SSP、または「1」などの簡易コンポーネント番号（ポートまたはモジュールの番号）など、デバイスの物理コンポーネント命名構文に応じて異なります。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）インターフェイス ID（**gigabitethernet0/1** など）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。
サブインターフェイス	（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。

コマンド デフォルト

インターフェイスを指定しない場合、ASA 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。

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

コマンド履歴

リリース	変更内容
7.2(1)	VLAN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

このコマンドは、ハイ アベイラビリティを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。

```
ciscoasa# 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 7 : show interface detail の各フィールド に、各フィールドの説明を示します。

表 *10 : show ip address* の各フィールド

フィールド	説明
インターフェイス（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。
名前	**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。
サブネット マスク	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 サーバーから受信しました。

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。

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

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	インターフェイス ID（**gigabit ethernet0/1** など）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。
proxy	IPL テーブル内のプロキシ エントリを表示します。
server	IPL テーブル内のサーバー エントリを表示します。
サブインターフェイス	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。
summary	エントリの要約を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	新しいサーバー機能に適応するための **lease** キーワードおよび **server** キーワードが追加されました。

リリース	変更内容
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 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。
9.1(4)	新しいサーバー機能に適応するための proxy キーワードおよび summary キーワードが追加されました。

使用上のガイドライン

出力の説明については、「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。

```
ciscoasa# 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 7 : show interface detail の各フィールド に、各フィールドの説明を示します。

***表 11 : 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 サーバー アドレス。

フィールド	説明
state	DHCP リースの状態で、次のとおりです。 • Initial：初期化状態で、ASA 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：ASA は 1 つ以上の DHCP サーバーから 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：ASA は、要求を送信した送信先サーバー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、ASA はリースを削除します。 • Bound：ASA は有効なリースを保持し、正常に動作しています。 • Renewing：ASA 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 サーバーに定期的に送信し、応答を待機します。 • Rebinding：ASA は元のサーバーのリースを更新することに失敗したため、いずれかのサーバー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：ASA はリースを削除するプロセスを開始しました。 • Releasing：ASA 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ーに送信します。
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ーによって使用される乱数。
Lease	DHCP サーバー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。
Rebind	ASA が DHCP サーバー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、ASA が元の DHCP サーバーと通信できず、リース期間の 87.5% を経過した場合です。ASA 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 サーバーに接続を試みます。
Temp default-gateway addr	DHCP サーバーによって指定されるデフォルト ゲートウェイ アドレス。

フィールド	説明
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。
リトライ回数	ASA 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、ASA 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、ASA が Selecting 状態の場合、この値は ASA が探索メッセージを送信した回数を示します。ASA が Requesting 状態の場合、この値は ASA が要求メッセージを送信した回数を示します。
Client-ID	サーバー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。

```
ciscoasa# 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 7-12 に、各フィールドの説明を示します。

表 *12 : show ip address dhcp server* の各フィールド

フィールド	説明
DHCP サーバー	このインターフェイスがリースを取得した DHCP サーバーアドレス。最上位エントリ（「ANY」）はデフォルト サーバーで常に存在します。
Leases	サーバー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ー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	サーバーからのオファーの数。
Requests	サーバーに送信された要求の数。

フィールド	説明
Acks	サーバーから受信した確認応答の数。
Naks	サーバーから受信した否定応答の数。
Declines	サーバーから受信した拒否の数。
リリース	サーバーに送信されたリリースの数。
Bad	サーバーから受信した不良パケットの数。
DNS0	DHCP サーバーから取得したプライマリ DNS サーバー アドレス。
DNS1	DHCP サーバーから取得したセカンダリ DNS サーバー アドレス。
WINS0	DHCP サーバーから取得したプライマリ WINS サーバー アドレス。
WINS1	DHCP サーバーから取得したセカンダリ WINS サーバー アドレス。
Subnet	DHCP サーバーから取得したサブネット アドレス。
DNS ドメイン	DHCP サーバー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 サーバーから 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	インターフェイス ID（**gigabitethernet0/1** など）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。
サブインターフェイス	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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、「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。

```
ciscoasa# 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 サーバーから 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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。

```
ciscoasa# 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** コマンドの設定を表示します。

show ip local pool

IPv4 アドレスプール情報を表示するには、特権 EXEC モードで **show ip local pool** コマンドを使用します。

show ip local pool interface *pool_name*

構文の説明

pool_name アドレス プールの名前。プールのリストを確認するには、? を入力します。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用し、**ip local pool** コマンドで作成した IPv4 アドレスプールの内容を表示します。これらのプールは、リモートアクセス VPN およびクラスタリングで使用されます。IPv6 アドレスプールを表示するには、**ipv6 local pool** コマンドを使用します。

例

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

```
ciscoasa# show ip local pool test-ipv4-pool

Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0
Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

関連コマンド

コマンド	説明
ip local pool	IPv4 アドレス プールを設定します。

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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# 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** の設定をクリアします。
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。

コマンド	説明
show running-config ip verify reverse-path	**ip verify reverse-path** の設定を表示します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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。

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

次に、**show ips detail** コマンドの出力例を示します。

```
ciscoasa# 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	AIP SSM へトラフィックを誘導します。

show ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec df-bit** コマンドを使用します。同じ意味を持つ **show crypto ipsec df-bit** コマンドも使用できます。

show ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

d f ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
ciscoasa(config)# show
 ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの IPsec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec fragmentation** コマンドを使用します。同じ意味を持つ **show crypto ipsec fragmentation** コマンドも使用できます。

show ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンドインターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、グローバル コンフィギュレーション モードで、inside という名前のインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
ciscoasa(config)# show ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show ipsec policy

OSPFv3 に設定されている IPsec セキュアソケット API（SS API）セキュリティポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec policy** コマンドを使用します。このコマンドの代替形式である **show crypto ipsec policy** を使用することもできます。

show ipsec policy

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。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
ciscoasa# show ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 123456789012345678901234567890123
Outbound ESP Cipher Key: 123456789012345678901234567890123
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

コマンド	説明
ipv6 ospf encryption	OSPFv3 の認証と暗号方式ポリシーを設定します。
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3インターフェイスに関する情報を表示します。

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。このコマンドの代替形式である **show crypto ipsec sa** を使用することもできます。

show ipsec sa [**assigned-address** *hostname* または *IP address* **| entry | identity | inactive | map** *map-name* **| peer** *peer-addr*] [**detail**]

構文の説明

assigned-address	（オプション）指定されたホスト名または IP アドレスの IPsec SA を表示します。
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	（オプション）IPsec SA をピア アドレスの順に表示します。
identity	（オプション）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。
inactive	（オプション）トラフィックを渡すことができない IPsec SA を表示します。
map *map-name*	（オプション）指定されたクリプト マップの IPsec SA を表示します。
peer *peer-addr*	（オプション）指定されたピア IP アドレスの IPsec SA を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.0(1)	OSPFv3 およびマルチ コンテキスト モードのサポートが追加されました。
9.1(4)	割り当てられた IPv6 アドレスを反映し、IKEv2 デュアルトラフィックの実行時に、GRE トランスポート モードのセキュリティ アソシエーションを示すように、出力が更新されました。

例

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには、割り当てられた IPv6 アドレス、およびトランスポート モードと GRE カプセル化の表示が含まれます。

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4
     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには使用中の設定が含まれ、トンネルが OSPFv3 として示されています。

```
ciscoasa(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 ={L2L, Transport, Manual key (OSPFv3),}
         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 ={L2L, Transport, Manual key (OSPFv3), }
         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)
ciscoasa(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 ポリシーに、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。

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry** に対する IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry detail** を使用して IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
ciscoasa(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** を使用した IPsec SA の例を示します。

```
ciscoasa(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
```

次の例では、IPv6 で割り当てられたアドレスに基づいて IPSec SA を表示しています。

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
 rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35
      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

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。
isakmp enable	IPsec ピアが ASA 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

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

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

```
ciscoasa(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
ciscoasa(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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ESPv3 統計情報が IPSec サブシステムとともに示され、マルチ コンテキスト モードのサポートが追加されました。

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、ASA 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）。
着信	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。

出力	説明
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。
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。
発信	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。

出力	説明
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。
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。

出力	説明
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。

```
ciscoasa(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
```

IPsecフローオフロードをサポートするプラットフォームでは、出力にはオフロードフローのカウンタが表示され、通常のカウンタにはオフロードフローと非オフロードフローの合計が表示されます。

```
ciscoasa# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。