show s - sz

show sctp

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

show sctp ［**detail**］

構文の説明

detail	SCTP アソシエーションに関する詳細情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

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

Management Center から FlexConfig を使用して SCTP インスペクションを有効にすると、このコマンドで SCTP 情報を表示できます。

例

次に、**show sctp** コマンドの出力例を示します。

```
> show sctp

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

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

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

```
> show sctp detail

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

関連コマンド

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

show serial-number

プリント基板（PCB）のシリアル番号を表示するには、**show serial-number** コマンドを使用します。このコマンドは仮想デバイスでは使用できません。

show serial-number

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show serial-number コマンドを使用して、プリント基板のシリアル番号を表示します。この情報は、**show version system** および **show running-config** の出力にも表示されます。

show inventory コマンドを使用して、シャーシのシリアル番号を表示します。

例

次に、シリアル番号を表示する例を示します。この例の番号は無効な番号に変更されています。

```
> show serial-number
XXX175078X5
```

show service-policy

サービスポリシーの統計情報を表示するには、**show service-policy** コマンドを使用します。

show service-policy ［**global** | **interface** *intf*］［**cluster flow-mobility** | **inspect** *inspection* ［*arguments*］ | **police** | **priority** | **set connection** ［**details**］ | **sfr** | **shape** | **user-statistics**］
show service-policy ［**global** | **interface** *intf*］［**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} ［**eq** *src_port*］ {**host** *dest_host* | *dest_ip dest_mask*} ［**eq** *dest_port*］［*icmp_number* | *icmp_control_message*］］

構文の説明

cluster flow-mobility	（オプション）脅威に対する防御 クラスタのフローモビリティに関するステータス情報を表示します。
dest_ip dest_mask	**flow** キーワードの場合、宛先 IP アドレスおよびトラフィックフローのネットマスク。
details	（オプション）**set connection** キーワードの場合、クライアントごとの接続制限が有効な場合に、クライアントごとの接続情報を表示します。
eq *dest_port*	**flow** キーワードの場合、フローの宛先ポートに相当します。
eq *src_port*	（オプション）**flow** キーワードの場合、フローの送信元ポートに相当します。
flow *protocol*	（オプション）5つのタプル（プロトコル、送信元IPアドレス、送信元ポート、宛先 IP アドレス、宛先ポート）で識別される特定フローに一致するポリシーを示します。このコマンドを利用すると、サービス ポリシー コンフィギュレーションによって、必要なサービスが特定の接続に提供されることを確認できます。
global	（オプション）出力をグローバル ポリシーに制限します。
host *dest_host*	**flow** キーワードの場合、トラフィックフローのホスト宛先 IP アドレス。
host *src_host*	**flow** キーワードの場合、トラフィックフローのホスト送信元 IP アドレス。
icmp_control_message	（オプション）プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィックフローの ICMP 制御メッセージを指定します。
icmp_number	（オプション）プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィックフローの ICMP プロトコル番号を指定します。

inspect *inspection* [*arguments*]	（オプション）**inspect** コマンドを含むポリシーに関する詳細情報を表示します。詳細出力では、一部の **inspect** コマンドはサポートされません。すべてのインスペクションを表示するには、**show service-policy inspect ?** コマンドを使用します。各インスペクションで使用できる引数は異なります。詳細については、CLIヘルプを参照してください。
interface *intf*	（オプション）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* はインターフェイス名です。
police	（オプション）**police** コマンドを含むポリシーに関する詳細情報を表示します。
priority	（オプション）**priority** コマンドを含むポリシーに関する詳細情報を表示します。
set connection	（オプション）**set connection** コマンドを含むポリシーに関する詳細情報を表示します。
sfr	（オプション）ASA Firepower モジュールのポリシーに関する詳細情報を表示します。このキーワードは 脅威に対する防御 には有効ではありません。
shape	（オプション）**shape** コマンドを含むポリシーに関する詳細情報を表示します。
src_ip src_mask	**flow** キーワードの場合、送信元IPアドレスおよびトラフィックフローで使用されるネットマスク。
user-statistics	（オプション）**user-statistics** コマンドを含むポリシーに関する詳細情報を表示します。このキーワードは 脅威に対する防御 には有効ではありません。

コマンド デフォルト

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

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show service-policy コマンドの出力に表示される初期接続の数は、特定のトラフィッククラスに関して定義されたトラフィックマッチング用のインターフェイスに対する初期接続の現在の数を示しています。「embryonic-conn-max」フィールドには、トラフィッククラスに設定された最大初期接続の制限値が表示されます。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続がトラフィックに一致すると、その接続に対して TCP 代行受信が適用されます。

コンフィギュレーションに対してサービスポリシーの変更を加えた場合は、すべての新しい接続で新しいサービスポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータが含まれていません。すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** コマンドまたは **clear local-host** コマンドを参照してください。

Management Center または Device Manager を使用してサービスポリシーを直接設定することはできません。さまざまな接続設定を編集したり、QoS ポリシーを設定したりすると、一部が間接的に変更されます。**configure inspection** コマンドを使用して、有効にするデフォルトのインスペクションを調整することもできます。Management Center で FlexConfig を使用してサービスポリシーを設定する場合、このコマンドは設定に関連した統計を表示します。

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

例

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

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
```

```
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

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

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

次に、GTP インスペクションの統計情報を表示するコマンドを示します。出力については、例に続く表の中で説明します。

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

表 *1 : GPRS GTP* 統計情報

カラムのヘッダー	説明
version_not_support	サポートされていない GTP バージョン フィールドを持つパケットの数を表示します。
msg_too_short	長さが 8 バイトより短いパケットの数を表示します。
unknown_msg	不明なタイプのメッセージ数を表示します。
unexpected_sig_msg	予期しないシグナリング メッセージ数を表示します。
unexpected_data_msg	予期しないデータ メッセージ数を表示します。
mandatory_ie_missing	必須情報要素（IE）が欠落しているメッセージ数を表示します。
mandatory_ie_incorrect	不正な形式の必須情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	無効なオプション情報要素（IE）を持つメッセージ数を表示します。
ie_unknown	不明な情報要素（IE）を持つメッセージ数を表示します。
ie_out_of_order	順番どおりでない情報要素（IE）を持つメッセージ数を表示します。
ie_unexpected	予期しない情報要素（IE）を持つメッセージを表示します。
ie_duplicated	重複した情報要素（IE）を持つメッセージ数を表示します。
optional_ie_incorrect	不正な形式のオプション情報要素（IE）を持つメッセージ数を表示します。
total_dropped	ドロップされたメッセージの合計数を表示します。
signalling_msg_dropped	ドロップされた信号メッセージ数を表示します。
data_msg_dropped	ドロップされたデータ メッセージ数を表示します。
total_forwarded	転送されたメッセージの合計数を表示します。
signalling_msg_forwarded	転送された信号メッセージ数を表示します。
data_msg_forwarded	転送されたデータ メッセージ数を表示します。
total created_pdp	作成されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。

カラムのヘッダー	説明
total deleted_pdp	削除されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	これらのフィールドは、実装機能である PDP マスター制御ブロックの使用に関連しています。これらのカウンタは、トラブルシューティング向けにシスコテクニカルサポートによって使用され、エンドユーザーには直接の関係はありません。
pdp_non_existent	存在しない PDP コンテキストに対して受信したメッセージ数を表示します。

次に、PDP コンテキストに関する情報を表示するコマンドを示します。

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

次の表で、**show service-policy inspect gtp pdp-context** コマンドの出力について説明します。

表 *2 : PDP* コンテキスト

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

関連コマンド

Command	説明
clear service-policy	サービスポリシーの統計情報をすべてクリアします。
configure inspection	デフォルトの検査を有効または無効にします。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show shun

回避情報を表示するには、**show shun** コマンドを使用します。

show shun ［*src_ip* | **statistics**］

構文の説明

src_ip	（任意）このアドレスに関する情報を表示します。
statistics	（任意）インターフェイスの回避統計を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show shun** コマンドの出力例を示します。

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

関連コマンド

Command	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。

show sip

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

show sip

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show sip コマンドは、脅威に対する防御 デバイスを越えて確立されている SIP セッションの情報を表示します。

例

次に、**show sip** コマンドの出力例を示します。

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

次の例では、脅威に対する防御 デバイス上の 2 つの SIP セッションが表示されています（Total フィールドを参照）。各 call-id が 1 つのコールを表します。

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

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

関連コマンド

コマンド	説明
show conn	さまざまな接続タイプの接続状態を表示します。

show skinny

SCCP（Skinny）セッションに関する情報を表示するには、**show skinny** コマンドを使用します。

show skinny ［**audio** | **video**］

構文の説明

audio	SCCP オーディオセッションの表示
video	SCCP ビデオセッションの表示

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、次の条件における **show skinny** コマンドの出力例を示します。デバイスを越えて 2 つのアクティブな Skinny セッションが設定されています。最初の Skinny セッションは、ローカルアドレス 10.0.0.11 にある内部 Cisco IP 電話と 172.18.1.33 にある外部 Cisco Unified Communications Manager の間に確立されています。TCP ポート 2000 は Cisco Unified Communications Manager です。2 番目の Skinny セッションは、ローカルアドレス 10.0.0.22 にある別の内部 Cisco IP 電話と同じ Cisco Unified Communications Manager の間に確立されています。

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力から、両方の内部 Cisco IP Phone の間でコールが確立されていることがわかります。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

関連コマンド

コマンド	説明
show conn	さまざまな接続タイプの接続状態を表示します。

show sla monitor

インターネット プロトコル サービス レベル契約（IP SLA）に関する情報を表示するには、**show sla monitor** コマンドを使用します。

show sla monitor {**configuration** | **operational-state**} [*sla_id*]

構文の説明

configuration	SLA の設定値（デフォルト値を含む）を表示します。
operational-state	SLA 動作の動作状態を表示します。
sla_id	（任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。

コマンド デフォルト

SLA ID が指定されていない場合は、すべての SLA 動作の設定値が表示されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、**show sla monitor configuration** コマンドの出力例を示します。SLA 動作 124 の設定値が表示されます。**show sla monitor configuration** コマンドの出力に続いて、同じ SLA 動作の **show running-config sla monitor** コマンドの出力が表示されます。

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
> show running-config sla monitor 124

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

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

```
> show sla monitor operational-state

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

関連コマンド

Command	説明
show running-config sla monitor	実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。

show snmp-server

デバイスで設定されたSNMPサーバーの情報を表示するには、**show snmp-server**コマンドを使用します。

show snmp-server {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

構文の説明

engineID	SNMP エンジンの ID を表示します。
group	設定されている SNMP グループの名前、使用するセキュリティモデル、さまざまなビューのステータス、および各グループのストレージタイプを表示します。
host	ホストグループに属する設定済みの SNMP ホストの名前、使用されているインターフェイスおよび使用されている SNMP のバージョンを表示します。
statistics	SNMP サーバー統計情報を表示します。
user [*username*]	SNMP ユーザーの特性に関する情報を表示します。必要に応じて、ユーザー名を指定して、そのユーザーに情報を制限できます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

SNMP エンジンは、ローカル デバイス上に配置できる SNMP のコピーです。エンジン ID は、各 SNMP エージェントごとに割り当てられる固有の値です。エンジン ID は設定できません。エンジン IDの長さは25バイトで、このIDは暗号化されたパスワードの生成に使用されます。フェールオーバー ペアでは、エンジン ID がピアと同期化されます。

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

（注） 統計には、SNMPモジュールへの入出力パケットに関する情報が表示されます。パケットが出力されたからといって、宛先に到達したということではありません。ルートの問題、介在するファイアウォール、接続されていないインターフェイスなどにより、出力パケットの送信が妨げられる可能性があります。パケットが SNMP サーバーに到達していない場合は、**show asp drop** や **show logging** などのコマンドを使用して他の問題を確認します。

例

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

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

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

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

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

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

次に、デバイスをポーリングしているアクティブなホストのみを表示する **show snmp-server host** コマンドの出力例を示します。

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

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

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

この出力には次の情報が表示されます。

- ユーザー名。SNMP ユーザーの名前を識別するストリングです。
- エンジン ID。デバイス上の SNMP のコピーを識別する文字列です。
- ストレージタイプ。デバイスの揮発性メモリまたは一時メモリに設定が格納されているか、あるいは不揮発性メモリまたは永続メモリに格納されているかを示します。非揮発性メモリまたは永続メモリに格納されている場合、デバイスをオフにして再度オンにした場合でも設定は存続します。

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

関連コマンド

Command	説明
clear snmp-server statistics	SNMP パケットの入力カウンタおよび出力カウンタをクリアします。
show running-config snmp-server	SNMP サーバー コンフィギュレーションを表示します。

show snort counters

Snortプリプロセッサ接続の統計情報を表示するには、**show snort counters** コマンドを使用します。

show snort counters {**action** | **stream** | **sip** | **ssl** | **smtp** | **vrf**} {**all** | **instance***x*}

構文の説明

action	アクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示します。
stream	ストリームプリプロセッサの統計情報を表示します。
sip	SIP プリプロセッサの統計情報を表示します。
ssl	SSL プリプロセッサの統計情報を表示します。
smtp	SMTP プリプロセッサの統計情報を表示します。
vrf	各仮想ルータを通過するライブセッションの数を表示します。
all	システム内のすべての Snort インスタンスの統計情報を表示します。たとえば、**show snort counters action all**、**show snort counters smtp all** などです。
instance*x*	システム内の選択した Snort インスタンスの統計情報を表示します。たとえば、**show snort counters smtp instance 11** のようになります。使用可能なインスタンス番号を確認するには、**show snort instances** コマンドを使用します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。
6.6	**vrf** キーワードが追加されました。

使用上のガイドライン

システムの Snort インスタンスの統計情報を表示するには、このコマンドを使用します。これらの統計情報は、情報提供やデバッグの目的で使用できます。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。**show snort counters action all** コマンドを使用して、システム内のすべての Snort インスタンスのアクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示します。使用可能なインスタンス番号を確認するには、**show snort instances** コマンドを使用します。

次に、システム内のすべての Snort インスタンスのアクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示する例を示します。

```
> show snort counters action all
Instance : 1
------------

Action Stats are not available
 Total Action Processed:           0

...

================================================================================

Instance : 16
------------

Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       220009 (100.000%)
      Block:         5076 (  2.307%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)

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

次に、スチーム統計情報の例を示します。

```
> show snort counters stream all
Instance : 1
------------

Stream statistics not available
 Total sessions: 0
================================================================================

...

Instance : 16
------------

Stream statistics:
            Total sessions: 665
              TCP sessions: 665
              UDP sessions: 0
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
```

```
                IP Prunes: 0
TCP StreamTrackers Created: 0
TCP StreamTrackers Deleted: 0
              TCP Timeouts: 661
              TCP Overlaps: 0
       TCP Segments Queued: 0
     TCP Segments Released: 0
       TCP Rebuilt Packets: 0
         TCP Segments Used: 0
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 0
      UDP Sessions Deleted: 0
              UDP Timeouts: 0
              UDP Discards: 0
                    Events: 0
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                Inspected: 0
                  Tracked: 910736
           UDP Port Filter
                  Filtered: 0
                Inspected: 0
                  Tracked: 0

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

次に、Snort インスタンス 1 の SMTP 統計情報の例を示しています。

```
> show snort counters smtp instance 1
Instance : 1
------------

SMTP Preprocessor Statistics
  Total sessions                                    : 80
  Max concurrent sessions                           : 1
  Base64 attachments decoded                        : 0
  Total Base64 decoded bytes                        : 0
  Quoted-Printable attachments decoded              : 0
  Total Quoted decoded bytes                        : 0
  UU attachments decoded                            : 0
  Total UU decoded bytes                            : 0
  Non-Encoded MIME attachments extracted            : 0
  Total Non-Encoded MIME bytes extracted            : 0

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

関連コマンド

Command	説明
clear snort statistics	Snort インスペクションの統計情報をクリアします。
show snort statistics	Snortによってトラフィックが検査されたときに、さまざまなSnort判定で一致したパケットの数を表示します。
show snort tls-offload	ハードウェアの検査エンジン（Snort）によって暗号化および復号化されたパケット関連の統計情報を表示します。

show snort instances

他の **show snort** コマンドで使用できる Snort インスタンス番号のリストを表示するには、**show snort instances** コマンドを使用します。

show snort instances

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、Snort インスタンスのリストを表示する例を示します。

```
> show snort instances
Total number of instances available - 2

+----------+---------+
| INSTANCE |   PID   |
+----------+---------+
|    1     |   2787  |
|    2     |   2788  |
+----------+---------+
```

show snort preprocessor-memory-usage

Snortインスタンスごとの Snortプリプロセッサのメモリ使用状況の統計情報を表示するには、**show snort preprocessor-memory-usage** コマンドを使用します。

show snort preprocessor-memory-usage *instance_ID* {**all** | **imap** | **pop** | **smtp**}

構文の説明

instance_ID	Snortインスタンスの ID 番号。システムでアクティブなインスタンス ID 番号のリストを取得するには、**show snort instances** コマンドを使用します。
all	すべてのプリプロセッサの統計情報を表示します。
imap	IMAP プリプロセッサの統計情報のみを表示します。
pop	POP プリプロセッサの統計情報のみを表示します。
smtp	SMTP プリプロセッサの統計情報のみを表示します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、Snortインスタンス 1 の SMTP プリプロセッサの統計情報を表示する例を示します。管理者パスワードの入力を求められます。

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
----------------------------------


Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
       Total Sessions seen: 0
   Max concurrent sessions: 0
   Current Active sessions: 0

   Memory Pool:
```

```
        Free Memory:
            SMTP Mime Pool:       17968000 bytes
                 SMTP Pool:              0 bytes
        Used Memory:
            SMTP Mime Pool:              0 bytes
                 SMTP Pool:              0 bytes
        -------------------       ---------------
        Total Memory:             17968000 bytes

   Heap Memory:
                    Session:              0 bytes
              Configuration:          16784 bytes
              --------------         ------------
               Total Memory:          16784 bytes
               No of allocs:             38 times
                IP sessions:             30 times
-----------------------------------------------------
```

show snort statistics

Snortによってトラフィックが検査されたときに、さまざまなSnort判定で一致したパケットの数を表示するには、**show snort statistics** コマンドを使用します。

show snort statistics

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、アクセスポリシー設定と侵入ルール設定に関する Snort インスペクションの結果を表示します。このコマンドは通常、予期しない Snort インスペクション動作をデバッグするときに使用されます。統計には、次の情報が含まれています。

- Passed Packets：Lina から Snort に送信されたパケットの数。
- Blocked Packets：Lina でブロックされ、Snort に送信されなかったパケットの数。
- Injected Packets：Snort が作成し、トラフィックストリームに追加したパケットの数。たとえば、リセットアクションを伴うブロックを設定すると、Snort は接続をリセットするためのパケットを生成します。
- Packets bypassed（Snort Down or Snort Busy）：Snort インスペクションを必要とするパケットを許可するようにシステムを設定しているものの、Snort がインスペクションを実行できない場合、これらのカウンタには、Snort がダウンしているかビジー状態であるためにパケットを処理できないときにインスペクションをバイパスしたパケットの数が表示されます。

⚠

注意 フローがバイパスされる（インスペクションなしで渡される）と、これらのビジーカウンタおよびダウンカウンタは、バイパスされたセッションが終了するまで増加し続けます。この増加は、Snortがビジーまたはダウン状態ではなくなってからも続く場合があります。たとえば、数日間続く持続的な TCP 接続が、Snort がビジーまたはダウン状態の間もパケットを送信する場合、カウンタは数日間増加を続け、Snort が再開した後も増加し続けます。

- Fast-forwarded flows：ポリシーによって高速転送されたため、検査されなかったフローの数。
- Blacklisted flows：Snort によってドロップされた、ポリシー設定からのフローの数。
- Start-of-flow events：Lina プロセスは、フローを Snort に送信せずに高速パスするときに、Snort にフロー開始イベントを送信します。これらのイベントは、Snort が接続を追跡し、接続イベントを報告するのに役立ちます。

- End-of-flow events：高速パスフローが終了すると、Lina プロセスはフロー終了イベントを Snort に送信します。
- Denied flow events：Lina プロセスは、Snort に送信する前にフローをドロップすることを決定すると、拒否されたフローイベントを Snort に送信します。
- Frames forwarded to Snort before drop：NGIPS インターフェイスのみで有効です。これは Snort に転送されドロップされたパケットの数です。Lina プロセスが何らかの理由（無効な TCP ヘッダー長、無効な UDP 長、無効な IP 長）でフレームをドロップすることに決定すると、可視性のため、フレームが Snort にも送信されます。
- Inject packets dropped：Snort がトラフィックストリームに追加したパケットのうち、ドロップされたパケット数。

例

次のサンプルトランスクリプトは、**show snort statistics** コマンドによって表示される情報を示しています。

```
show snort statistics
Packet Counters:
  Passed Packets                                     6
  Blocked Packets                                    321
  Injected Packets                                   284
  Packets bypassed (Snort Down)                      0
  Packets bypassed (Snort Busy)                      0

Flow Counters:
  Fast-Forwarded Flows                               0
  Blacklisted Flows                                  0

Miscellaneous Counters:
  Start-of-Flow events                               0
  End-of-Flow events                                 0
  Denied flow events                                 0
  Frames forwarded to Snort before drop              0
  Inject packets dropped                             0
```

次の例では、すべてのトラフィックをブロックしてリセットするようにアクセス コントロール ポリシーが設定されている場合について考慮します。Lina はリセットを処理できないため、パケットを Snort に渡して、クライアントとサーバー両方へのリセットをブロックおよび送信させます。

- Passed packets：Lina から Snort に渡された 8 つのパケットを表示します。
- Injected packets：クライアントとサーバーに送信された 2 つのパケットを表示します。
- Blacklisted flows：Snort が Lina にブロックするように指示したフローを表示します。

（注） この例では、*blocked* パケットは存在しません。

```
> show snort statistics
Packet Counters:
  Passed Packets                                         8
  Blocked Packets                                        0
  Injected Packets                                       2
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      3

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

次の例では、アクセス コントロール ポリシーに、FTP ポートに一致する 1 つのルールとブロックアクションがあり、HTTP アプリケーションに一致する別のルールと許可アクションが存在する場合について考慮します。

- Passed packets：Lina が許可ルールのパケットを Snort に送信するため、60 個の HTTP パケットが表示されます。
- Denied flow events：FTP ポート照合で Lina が処理した 2 つのデータおよび制御チャネルパケットを表示します。

（注） この例では、*blocked* パケットは存在しません。

```
> show snort statistics
Packet Counters:
  Passed Packets                                        60
  Blocked Packets                                        0
  Injected Packets                                       0
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     2
  Frames forwarded to Snort before drop                  0
```

```
Inject packets dropped                                    0
```

関連コマンド

Command	説明
clear snort statistics	Snort インスペクションの統計情報をクリアします。
configure snort preserve-connection	Snort プロセスがダウンした場合に、ルーテッドインターフェイスとトランスペアレント インターフェイスで既存の TCP/UDP 接続を維持するかどうかを指定します。

show snort tls-offload

ハードウェアの検査エンジン（Snort）によって暗号化および復号化されたパケット関連の統計情報を表示するには、**show snort tls-offload** コマンドを使用します。このコマンドは、SSL ハードウェア アクセラレーションをサポートする次の管理対象デバイスでのみ使用できます。

- Threat Defense を搭載した Firepower 2100
- を搭載した Firepower 4100/9300 Threat Defense

  Firepower 4100/9300 Threat Defense コンテナインスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

show snort tls-offload [proxy | tracker | description]

構文の説明

proxy	（オプション）プロキシの統計情報のみを表示します。
tracker	（オプション）トラッカーの統計情報のみを表示します。
description	（オプション）プロキシとトラッカーの両方のカウンタの説明を表示します。

コマンド履歴

リリース	変更内容
6.2.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、Snort のプロキシおよびトラッカーコンポーネントの詳細な統計情報を表示します。これらの統計情報は、情報提供やデバッグの目的で使用できます。カウンタの説明を表示するには、**show snort tls-offload description** コマンドを使用します。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

次に、**show snort tls-offload** コマンドの例を示します。

```
====== Tracker Statistics ======
TOTAL_CONNECTION                  2774
TOTAL_RSA_KEY_EXCHANGE_4K         2774
TOTAL_CIPHER_SUITE_ENCR_AES       2774
TOTAL_CIPHER_SUITE_HASH_SHA1      2774
TOTAL_CKE_PMS_DECRYPTED           2774
TOTAL_RECORD_DECRYPTED            363001
TOTAL_RECORD_ENCRYPTED            363001
TOTAL_CONNECTION_W_DUR (<0.5s)    2771
AVG_CONNECTION_DURATION   (ms)    184
AVG_HANDSHAKE_TIME        (ms)    37
AVG_CKE_PMS_DECRYPT_TIME (us)     21402
```

```
AVG_RECORD_DECRYPT_TIME  (us)    619
AVG_RECORD_ENCRYPT_TIME  (us)    477
PEAK_CONNECTION_DURATION (ms)    400
PEAK_HANDSHAKE_TIME      (ms)    62
CONCURRENT_CONNECTION/Peak       3/3
CPS_ATTEMPTED/Peak               7/8
CPS_COMPLETED/Peak               8/8
CKE_PMS_DECRYPTING_Q/Peak        0/2
SKE_DH_PARAM_SIGNING_Q/Peak      0/0
RECORD_ENCRYPTING_Q/Peak         1/25
RECORD_DECRYPTING_Q/Peak         1/2
======= Proxy Statistics =======
TOTAL_CONNECTION(LW+FP)          15855
TOTAL_CONNECTION_FP              15853
CONNECTION_FP_RECV_FIN           31697
CONNECTION_FP_RECV_RST           27
CONNECTION_LW_RECV_FIN           2
CONCURRENT_CONNECTION_LW/Peak    0/2
CONCURRENT_CONNECTION_FP/Peak    3/7
BYPASS_NOT_ENOUGH_MEM            0
```

関連コマンド

Command	説明
clear snort tls-offload	統計カウンタをクリアします。
debug snort tls-offload	すべてのSnortプロセスのすべてのタイプのエラーデバッグメッセージを表示します。

show software authenticity

ソフトウェアの真正性情報を表示するには、**show software authenticity** コマンドを使用します。

show software authenticity {**development** | **file** *filename* | **keys** | **running**}

構文の説明

development	開発キー署名付きイメージのロードが有効か無効かを表示します。
file *filename*	特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示します。
keys	SPI フラッシュに保存されている開発キーとリリースキーに関する情報を表示します。
running	現在実行中のイメージファイルのソフトウェア認証に関連したデジタル署名情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ファイルおよび実行中のイメージの出力には、次の情報が含まれています。

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

例

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

```
> show software authenticity development
Loading of development images is disabled
```

次に、**show software authenticity file** コマンドの出力例を示します。この例では、ファイルは開発イメージです。デバイスで現在実行中のイメージファイルに関して、**show software authenticity running** と同じ出力が表示されます。

```
> show software authenticity file os.img
File Name                     : disk0:/os.img
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

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

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

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

関連コマンド

Command	説明
show version	ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示します。

show ssd

SSD のステータスを表示するには、**show ssd** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

show ssd

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

例

次の表示例は、SSD に関する情報を示しています。

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

関連コマンド

Command	説明
configure raid	SSD を RAID に追加または RAID から削除します。
show raid	RAID ステータスを表示します。

show ssh-access-list

管理インターフェイスの SSH アクセスリスト設定を表示するには、**show ssh-access-list** コマンドを使用します。

show ssh-access-list

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

使用上のガイドライン

管理インターフェイスの SSH アクセスリスト設定を表示するには、このコマンドを使用します。アクセスリストにより、ユーザーが管理 IP アドレスへの SSH 接続を試行できる IP アドレスが決定されます。このリストは、データインターフェイスへの SSH アクセスを制御しません。

例

次に、**show ssh-access-list** コマンドからのデフォルトの出力例を示します。このアクセスリストは、任意の IP アドレスから管理 IP アドレスへの SSH 接続を許可します。実際に SSH 接続を完了するには、あらゆるユーザーが有効なユーザー名/パスワードを入力する必要があります。

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

関連コマンド

Command	説明
configure ssh-access-list	管理インターフェイスの SSH アクセスリストを設定します。

show ssl

アクティブな SSL セッションおよび使用可能な暗号に関する情報を表示するには、**show ssl** コマンドを使用します。

show ssl ［**cache** | **ciphers** ［*level*］ | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

構文の説明

cache	（オプション）SSLセッションキャッシュの統計情報を表示します。
ciphers	（オプション）使用可能な SSL 暗号を表示します。暗号強度を示す特定のレベルで使用可能な暗号のみを表示するには、level キーワードを含めます。考えられるレベルは次のとおりです（強度の昇順）。 • **all** • **low** • **medium** （レベルを指定しない場合のデフォルト） • **fips** • **high** （TLSv1.2 にのみ適用）
errors [**trace**]	（オプション）SSLエラーを表示します。各エラーのトレース情報を含めるには、trace キーワードを含めます。
mib [**64**]	（オプション）SSL MIB の統計情報を表示します。64 ビットカウンタの統計情報を表示するには、64 キーワードを含めます。
objects	（オプション）SSL オブジェクトの統計情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在の SSLv3 以上のセッションに関する情報を表示します。情報には、有効になっている暗号の順序、無効化された暗号、使用されている SSL トラストポイント、証明書認証が有効かどうかが含まれます。これらの設定は、管理インターフェイスではなく、データインターフェイスの SSL 接続用です。

例

次に、**show ssl** コマンドの出力例を示します。

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
```

```
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

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

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
```

```
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

show ssl-policy-config

現在適用されているSSLポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべてのSSLルールとルールの設定など）、信頼できるCA証明書、および復号化不可能なトラフィックのアクションを表示するには、**show ssl-policy-config** コマンドを使用します。

show ssl-policy-config

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

Management Center で SSL ポリシーを設定し、そのポリシーをデバイスに割り当てられたアクセス コントロール ポリシーにアタッチします。このコマンドを使用すると、デバイスを通過するトラフィックで SSL 復号化用に設定されたアクションに関する情報を表示できます。

例

次の例は、デバイスに SSL ポリシーを設定していない場合に表示される内容を示しています。

```
> show ssl-policy-config
SSL policy not yet applied.
```

次の例は、設定された SSL ポリシーを示しています。

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                              thawte-Primary-Root-CA
                              UTN-DATACorp-SGC
                              Chambers-of-Commerce-Root-2008
                              Izenpe.com-1
```

```
                                    A-Trust-Qual-02
                                    A-Trust-nQual-03
                                    Common-Policy
                                    Starfield-Root-Certificate-Authority-G2
                                    GeoTrust-Primary-Certification-Authority
                                    Certum-Trusted-Network-CA
                                    UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                    CA-Disig-Root-R1
                                    C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                    Thawte-Server-CA-1
                                   VeriSign-Class-3-Public-Primary-Certification-Authority-G3

                                    COMODO-Certification-Authority
                                   VeriSign-Class-3-Public-Primary-Certification-Authority-G5

                                    UTN-USERFirst-Client-Authentication-and-Email
                                    TC-TrustCenter-Universal-CA-III
                                    Cisco-Root-CA-2048
                                    Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

=============[ Undecryptable Actions ]==============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

関連コマンド

Command	説明
show access-policy-config	現在設定されているアクセス コントロール ポリシーに関する情報を表示します。

show ssl-protocol

ローカルデバイスマネージャ（Device Manager ）への HTTPS アクセス用に現在設定されている SSL プロトコルを表示するには、**show ssl-protocol** コマンドを使用します。

show ssl-protocol

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、管理インターフェイス用に設定されているSSLプロトコルを表示します。これらは、ローカルマネージャである Device Manager を開くために使用される HTTPS 接続用に許可されているプロトコルです。それらのSSLプロトコルは、リモートマネージャには使用されません。

SSL プロトコルを設定するには、**configure ssl-protocol** コマンドを使用します。

例

次に、ローカルマネージャを使用しているときに現在定義されている SSL プロトコルを表示する例を示します。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

関連コマンド

Command	説明
configure ssl-protocol	管理インターフェイスへの HTTPS アクセス用の SSL プロトコルを設定します。

show startup-config

スタートアップコンフィギュレーションを表示する、またはスタートアップコンフィギュレーションがロードされたときのエラーを表示するには、**show startup-config** コマンドを使用します。

show startup-config ［**errors**］

構文の説明

errors	（任意）スタートアップ コンフィギュレーションがロードされたときに生成されたエラーを表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show startup-config コマンドは、スタートアップシステム設定を表示します。これらのコマンドを直接設定することはできません。代わりに、デバイスを制御するマネージャ（Management Center や Device Manager など）で設定します。

ただし、これは部分的な設定です。ASA ソフトウェア コンフィギュレーション コマンドのみを使用して設定できる内容を示していますが、一部のコマンドは 脅威に対する防御 に固有のコマンドである場合があります。これらのコマンドは 脅威に対する防御 に移植されています。したがって、スタートアップ コンフィギュレーションの情報はトラブルシューティングの補助手段としてのみ使用してください。デバイスマネージャは、デバイス設定を分析する主な手段として使用します。

例

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

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names

(...Output Truncated...)
```

関連コマンド

Command	説明
show running-config	実行コンフィギュレーションを表示します。

show summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示するには、**show summary** コマンドを使用します。

show summary

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

サマリー情報には、基本的な **show version** の出力に加えて、適用されたポリシーと Snort バージョン情報のリストが含まれます。

例

次に、サマリー情報の表示例を示します。

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build
2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
-----------------------------------------------------

------------------[ policy info ]-------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

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

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
-----------------------------------------------------
```

show sunrpc-server active

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

show sunrpc-server active

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

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

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

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

関連コマンド

Command	説明
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールをクリアします。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。

show switch mac-address-table

スイッチのMACアドレステーブルを表示するには、**show switch mac-address-table** コマンドを使用します。

（注） Firepower 1010 でのみサポートされています。

show switch mac-address-table

コマンド履歴

リリース	変更内容
6.5	このコマンドが導入されました。

使用上のガイドライン

スイッチ MAC アドレス テーブルには、スイッチ ハードウェア内の各 VLAN のトラフィックに適用するMACアドレスとスイッチ ポートのマッピングが保持されます。このブリッジMACアドレス テーブルには、VLAN 間を通過するトラフィックに適用する MAC アドレスと VLAN インターフェイスのマッピングが保持されます。

MAC アドレス エントリは 5 分経過するとエージング アウトします。

例

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

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
 Mac Address | VLAN | Type | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 | dynamic | 287 | Et1/1
 0012.d927.fb03 | 0001 | dynamic | 287 | Et1/1
 0013.c4ca.8a8c | 0001 | dynamic | 287 | Et1/1
 00b0.6486.0c14 | 0001 | dynamic | 287 | Et1/1
 00d0.2bff.449f | 0001 | static | - | In0/1
 0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

次の表は、各フィールドの説明を示しています。

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

フィールド	説明
Mac Address	MAC アドレスを表示します。
VLAN	MAC アドレスに関連付けられている VLAN を表示します。

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

関連コマンド

Command	説明
show switch vlan	VLAN と物理 MAC アドレスの関連付けを表示します。

show switch vlan

VLAN および関連するスイッチポートを表示するには、**show switch vlan** コマンドを使用します。

（注） Firepower 1010 でのみサポートされています。

show switch vlan

コマンド履歴

リリース	変更内容
6.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。他のモデルの場合は、**show vlan** コマンドを使用します。

例

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

```
> show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                            up        Et1/1, Et1/2
200  outside                           up        Et1/8
300  -                                 down      Et1/2, Et1/3
400  backup                            down      Et1/4
```

次の表は、各フィールドの説明を示しています。

表 *4 : show switch vlan* のフィールド

フィールド	説明
VLAN	VLAN 番号を表示します。
名前	VLANインターフェイスの名前を表示します。名前が設定されていない場合、またはVLANインターフェイスがない場合は、ダッシュ（-）が表示されます。
Status（ステータス）	スイッチ内のVLANとトラフィックを送受信するためのステータス（upまたはdown）を表示します。VLANがアップ状態になるには、そのVLANで少なくとも1つのスイッチ ポートがアップ状態である必要があります。

フィールド	説明
ポート	各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN にリストされている場合、そのポートはトランク ポートです。上記の出力例で、Ethernet 1/2 は VLAN 100 および VLAN 300 を伝送するトランクポートです。

関連コマンド

Command	説明
show switch mac-address-table	スイッチ MAC アドレステーブルを表示します。

show tcpstat

TCP スタックおよびデバイスで終端している TCP 接続のステータスを（デバッグのために）表示するには、**show tcpstat** コマンドを使用します。

show tcpstat

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびデバイスで終端している TCP 接続のステータスを表示できます。次の表に、表示される TCP 統計情報の説明を示します。

表 *5 : show tcpstat* コマンドの *TCP* 統計情報

統計	説明
tcb_cnt	TCP ユーザーの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザー認可で使用されます。
tcp_xmt pkts	TCP スタックが送信したパケットの数。
tcp_rcv good pkts	TCP スタックが受信した正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	チェックサムに誤りがあった受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザーの数。
tcp user hash add dup	新しい TCP ユーザーをハッシュ テーブルに追加しようとしたとき、そのユーザーがすでにテーブル内に存在していた回数。
tcp user srch hash hit	検索時にハッシュ テーブル内でTCPユーザーが検出された回数。
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザーが検出されなかった回数。
tcp user hash delete	TCP ユーザーがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCPユーザーを削除しようとしたとき、そのユーザーがハッシュ テーブル内で検出されなかった回数。
lip	TCP ユーザーのローカル IP アドレス。
fip	TCP ユーザーの外部 IP アドレス。

統計	説明
lp	TCP ユーザーのローカル ポート。
fp	TCP ユーザーの外部ポート。
st	TCPユーザーの状態（RFC 793 を参照）。表示される値は次のとおりです。 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP ユーザーの再送信キューの長さ。
inqlen	TCP ユーザーの入力キューの長さ。
tw_timer	TCP ユーザーの time_wait タイマーの値（ミリ秒）。
to_timer	TCPユーザーの非アクティビティタイムアウトタイマーの値（ミリ秒）。
cl_timer	TCP ユーザーのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザーの持続タイマーの値（ミリ秒）。
rt_timer	TCP ユーザーの再送信タイマーの値（ミリ秒）。
tries	TCP ユーザーの再送信回数。

例

次に、TCP スタックのステータスを表示する例を示します。

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

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
```

```
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
  rt_timer = 0 tries 0
```

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

show tech-support

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

show tech-support

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.1	**show access-list element-count** および **show asp rule-engine** からの出力が追加されました。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。

例

次に、テクニカル サポート分析に使用される情報を表示する例を示します。出力は、先頭のみが表示されるように短縮されます。この出力は非常に長いため、結果が表示されるまでに時間がかかります。

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

show threat-detection memory

実行コンフィギュレーションで**threat-detection statistics**コマンドによって有効にされた高度な脅威検出統計情報で使用されるメモリを表示するには、**show threat-detection memory** コマンドを使用します。

show threat-detection memory

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

一部の統計情報は大量のメモリを使用して、システムのパフォーマンスに影響を与えることがあります。このコマンドを使用すると、必要に応じてコンフィギュレーションを調整できるようにメモリ使用率をモニターできます。

FlexConfig を使用して、**threat-detection statistics** コマンドを設定します。

例

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

```
> show threat-detection memory
Cached chunks:
       CACHE TYPE              BYTES USED
TD Host                          70245888
TD Port                              2724
TD Protocol                          1476
TD ACE                                728
TD Shared counters                  14256
============================
Subtotal TD Chunks               70265072


Regular memory                BYTES USED
TD Port                              33824
TD Control block                    162064
============================
Subtotal Regular Memory             195888


Total TD memory:                 70460960
```

Command	説明
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection statistics host	ホストの統計情報を表示します。

Command	説明
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。

show threat-detection rate

threat-detection basic-threatコマンドを使用して（FlexConfig を使用）基本的な脅威検出を有効にすると、**show threat-detection rate** コマンドを使用して統計情報を表示できます。

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

構文の説明

acl-drop	（任意）アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。
bad-packet-drop	（任意）パケット形式に誤りがあって（invalid-ip-header または invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレートを表示します。
conn-limit-drop	（任意）接続制限（システム全体のリソース制限および設定された制限の両方）を超えたためにドロップされたパケットのレートを表示します。
dos-drop	（任意）DoS 攻撃（無効な SPI やステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレートを表示します。
fw-drop	（任意）基本ファイアウォールチェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。interface-drop、inspect-drop、scanning-threat など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	（任意）疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。
inspect-drop	（任意）アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。
interface-drop	（任意）インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。
min-display-rate *events_per_second*	（任意）最小表示レート（1 秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。0 ～ 2147483647 の範囲で指定します。

scanning-threat	（任意）スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニターします。フルスキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
syn-attack	（オプション）TCP SYN 攻撃や戻りデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔。
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

システムは、平均レート間隔内でイベントカウントを30回計算します。つまり、システムは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が10分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 59 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

例

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

```
> show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
```

```
10-min  Scanning:                0          0      29                193
1-hour  Scanning:              106          0      10             384776
1-hour Bad  pkts:               76          0       2             274690
10-min  Firewall:                0          0       3                 22
1-hour  Firewall:               76          0       2             274844
10-min DoS attck:                0          0       0                  6
1-hour DoS attck:                0          0       0                 42
10-min Interface:                0          0       0                204
1-hour Interface:               88          0       0             318225
```

関連コマンド

Command	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection statistics	脅威検出の統計情報を表示します。

show threat-detection scanning-threat

（FlexConfig を使用して）**threat-detection scanning-threat** コマンドで脅威検出のスキャンを有効にした場合は、**show threat-detection scanning-threat** コマンドを使用して攻撃者およびターゲットとして分類されたホストを表示します。

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

構文の説明

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

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

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

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l21)
    192.168.1.249 (l21)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

関連コマンド

Command	説明
clear threat-detection scanning-threat	スキャンする脅威の攻撃者とターゲットのリストをクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection statistics	脅威検出の統計情報を表示します。
shun	脅威の攻撃者のスキャンなど、指定されたホストからの接続をブロックします。

show threat-detection shun

（FlexConfig を使用して）**threat-detection scanning-threat** コマンドで脅威検出のスキャンを有効にし、攻撃元ホストを自動的に回避した場合は、**show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

show threat-detection scanning-host

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

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

例

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

```
> show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

関連コマンド

Command	説明
clear threat-detection shun	自動的に回避されるホストのリストをクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection scanning-threat	スキャンする脅威の攻撃者とターゲットを表示します。
show threat-detection statistics	脅威検出の統計情報を表示します。
shun	脅威の攻撃者のスキャンなど、指定されたホストからの接続をブロックします。

show threat-detection statistics

threat-detection statistics コマンド（FlexConfig を使用）で脅威の統計情報を有効にする場合は、**show threat-detection statistics** コマンドを使用して統計情報を表示します。わかりやすくするため、次の図では主要なキーワードとオプションを個別に示しています。

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

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

show threat-detection statistics ［**min-display-rate** *eps*］ **protocol** ［*number* | *name*］

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

構文の説明

host [*ip_address* [*mask*]]	ホストの統計情報を表示します。必要に応じて、IPアドレスを指定して特定のホストの統計情報を表示できます。ホストのサブネットマスクを含めることができます。 FlexConfig を使用して **threat-detection statistics host** コマンドを設定し、ホストの統計情報を有効にします。
min-display-rate *eps*	（任意）最小表示レート（1 秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。0 ～ 2147483647 の範囲で指定します。
port [*start_port*[*-end_port*]]	TCP/UDPポートの統計情報を表示します。必要に応じて、単一のポートまたはポートの範囲（0 ー 65535）を指定できます。 FlexConfig を使用して **threat-detection statistics port** コマンドを設定し、ポートの統計情報を有効にします。
protocol [*number*	*name*]	プロトコルの統計情報を表示します。必要に応じて、数字または名前でプロトコルを指定できます。使用できる数字は 0ー255 です。次のいずれかの名前を使用できます。ah、eigrp、esp、gre、icmp、igmp、igrp、ip ipinip、ipsec、nos、ospf、pcp、pim、pptp、snp、tcp、udp FlexConfig を使用して **threat-detection statistics protocol** コマンドを設定し、プロトコルの統計情報を有効にします。

top [**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**]	統計情報を有効にしたオプションに応じて、上位10件のアクセスルール、ホスト、およびポート/プロトコルを表示します。次のキーワードを使用して、表示を絞り込むことができます。 • **access-list** 許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。**threat-detection basic-threat** コマンドを使用して基本脅威検出を有効にすると、**show threat-detection rate access-list** コマンドを使用してアクセスリストの拒否を追跡できます。 • **host** 一定期間ごとに上位 10 件のホスト統計情報を表示します。脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。 • **port-protocol** TCP/UDP ポートタイプと IP プロトコルタイプを組み合わせた上位 10 件の統計情報を表示します。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示に含まれていません。 • **rate-1**、**rate-2**、**rate-3** は、指定した固定レート期間の統計情報のみを表示します。指定できる最小間隔は 1、最大間隔は 3 です。たとえば、ディスプレイに直前の 1 時間、8 時間、および 24 時間の統計情報が表示されるとします。その場合、レート 1 は 1 時間、レート 2 は 8 時間、レート 3 は 24 時間を表します。
top tcp-intercept[**all**] [**detail**] [**long**]	TCP代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバーが含まれます。次のキーワードを含めることができます。 • **all** トレースされているすべてのサーバーの履歴データを表示します。 • **detail** 履歴サンプリングデータを表示します。 • **long** サーバーの実際の IP アドレスおよび変換後の IP アドレスとともに、統計情報の履歴を long 形式で表示します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

システムは、平均レート間隔内でイベントカウントを30回計算します。つまり、システムは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が20分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

次の表に、TCP代行受信の表示を除く、すべてのコマンドの出力を示します。この出力の説明については、TCP 代行受信の例を参照してください。

フィールド	説明
上 Name, ID	上位レポートの場合、この列にはアクセス制御エントリの名前または番号、ホストの IP アドレス、またはポートやプロトコルの名前/ID 番号が表示されます。 エントリは固定レート間隔でグループ化され、該当期間内で「0」（最大数）から「9」（最小数）にランク付けされます。10 の順位すべてについて十分な統計情報がない場合、指定した間隔に関して表示される項目が 10 未満になることがあります。 ホストおよびポートプロトコルの場合、グループ化は、固定間隔あたりの送受信済みバイト数およびパケット数に基づいて行われます。

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 システムは、各バースト期間の終わりにこの数を保存します。合計で 30 回分の完了したバースト間隔における数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に show コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に0です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

フィールド	説明
Entry heading	統計情報は、見出しの下に固定間隔でグループ化されます。見出しには、次の行で説明される情報を含めることができます。一般に、エントリの見出しは次の要素から始まります。 • ホスト、およびホスト IP アドレス。 • ポート番号やポート名。80/HTTP など。 • プロトコル番号またはプロトコル名。ICMP など。 • 上位レポートの場合、固定間隔および統計タイプ。アクセスリストの場合、見出しは表示が ACL ヒットに関するものであることを示します。
tot-ses	ホストがデータベースに追加された時点以降のホストにおける合計セッション数を表示します。
act-ses	ホスト、ポート、またはプロトコルが現在関係しているアクティブなセッションの合計数を表示します。
fw-drop （ホストのみ）	ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケットドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなしの UDP セッション攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop （ホストのみ）	アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。
null-ses （ホストのみ）	ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバーからデータの送信がなかった UDP セッションです。
bad-acc （ホストのみ）	閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌルセッション状態（上記を参照）であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。

フィールド	説明
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。 • Sent byte、Sent pkts：ホスト、ポート、またはプロトコルから正常に送信されたバイト数またはパケット数を表示します。 • Sent drop：スキャン攻撃の一部であったためにドロップされた、ホスト、ポート、またはプロトコルから送信されたパケット数を表示します。 • Recv byte、pkts：ホスト、ポート、またはプロトコルに正常に受信されたバイト数またはパケット数を表示します。 • Recv drop：スキャン攻撃の一部であったためにドロップされた、ホスト、ポート、またはプロトコルに受信されたパケット数を表示します。

例

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

```
> show threat-detection statistics host

                            Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0

  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
```

```
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

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

```
> show threat-detection statistics port

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

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

```
> show threat-detection statistics protocol

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

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

```
> show threat-detection statistics top access-list

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
  8-hour ACL hits:
              100/3[0]              21            1298       0               623488
              200/2[1]               5             326       0               156786
              100/1[2]               5             326       0               156786
```

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

```
> show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
```

```
 3         gopher   69              65              0       0          24345678
 4    Protocol-96 * 96              63              0       0          22345678
 5      Port-7314 7314              62              0       0          12845678
 6 BitTorrent/trc 6969              61              0       0          12645678
 7     Port-8191-65535              55              0       0          12345678
 8           SMTP  366              34              0       0           3345678
 9         IPinIP *  4              30              0       0           2345678
10          EIGRP * 88              23              0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

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

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

```
> show threat-detection statistics top host

                  Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938              0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28              0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9              0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697              0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29              0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42              0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367              0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3              0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3              0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337              0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3              0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14              0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122              0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1              0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112              0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1              0       0               104846
```

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

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
 Time)>
------------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

次の表で、TCP 代行受信の出力について説明します。

フィールド	説明
Monitoring window size	統計情報のためにシステムがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定は、FlexConfig を使用して **threat-detection statistics tcp-intercept rate-interval** コマンドで変更できます。システムは、この間隔でデータを 30 回サンプリングします。
Sampling interval	サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。
ランク	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバーで、10 位は最も攻撃が少なかったサーバーです。
Server IP:Port	攻撃を受けているサーバーの IP アドレスおよびポートを表示します。
インターフェイス	サーバーが攻撃を受けているインターフェイスを表示します。
Ave Rate	サンプリング期間中の攻撃の平均レートを 1 秒あたりの攻撃数で表示します。
Cur Rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
Total	攻撃の合計数を表示します。
Source IP	攻撃者の IP アドレスを表示します。
Last Attack Time	最後の攻撃が発生した時間を表示します。

次に、**show threat-detection statistics top tcp-intercept long** コマンドの出力例を示します。実際の IP アドレスが括弧内に表示されています

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total>
<Source IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

次に、サンプリングデータを表示する **show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。サンプリングデータは、30 のサンプリング期間あたりの攻撃数です。

```
> show threat-detection statistics top tcp-intercept detail

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

関連コマンド

Command	説明
clear threat-detection statistics	脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。

show time

デバイスのUTCおよびローカルの時刻と日付を表示するには、**show time** コマンドを使用します。

show time

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

例

次に、**show time** コマンドの出力例を示します。

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

show time-range

すべての時間範囲オブジェクトの設定を表示するには、**show time-range** コマンドを使用します。

（注） このコマンドは、デバイスの時刻を表示しません。デバイス時刻を表示するには、`show time` を使用します。

show time-range timezone ［ *name* ］

構文の説明

name	（オプション）この時間範囲オブジェクトの情報のみを表示します。
timezone	時間範囲ポリシーに設定されたタイムゾーンを表示するには、timezone を使用します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。
6.6	timezone キーワードが追加されました。

例

次に、時間範囲オブジェクトの設定を表示する例を示します。この例では、work-hours という名前のオブジェクトが 1 つあります。inactive は、オブジェクトが使用されていないことを意味します。

```
> show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

次に、**show time-range timezone** コマンドの出力例を示します。

```
> show time-range timezone
Time-range Clock:
------------------------------
13:20:22.852 tzname Tue Aug 18 2020
```

show tls-proxy

暗号化された検査の TLS プロキシおよびセッション情報を表示するには、**show tls-proxy** コマンドを使用します。

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

構文の説明

count	セッション カウンタだけを表示します。
detail [**cert-dump**]	各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。**cert-dump** キーワードを追加して、ローカルダイナミック証明書（LDC）の 16 進ダンプを取得します。 また、これらのキーワードは、**host** オプションとともに使用できます。
host *host_address*	関連付けられたセッションを表示する特定のホストの IPv4 または IPv6 アドレスを指定します。
session	アクティブな TLS プロキシ セッションを表示します。
statistics	TLS セッションをモニターおよび管理するための統計情報を表示します。
tls_name	表示する TLS プロキシの名前。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドで表示できる TLS プロキシは、暗号化されたアプリケーション検査用に設定されているプロキシだけです。プロキシは、SIP、SCCP（Skinny）、または Diameter インスペクションに適用されます。これらの TLS プロキシは、SSL 復号化または VPN ポリシーとは関係ありません。

例

次に、**show tls-proxy** コマンドの出力例を示します。

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
      Server proxy:
             Trust-point: local_ccm
      Client proxy:
             Local dynamic certificate issuer: ldc_signer
             Local dynamic certificate key-pair: phone_common
             Cipher-suite <unconfigured>
```

```
      Run-time proxies:
             Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
                   Active sess 1, most sess 4, byte 3244
```

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

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

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

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

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

```
> show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                        0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                             2
    SCCP:                                           20
    DIAMETER:                                      200
Total TLS Proxy Sessions
    Established:                                   822
    Platform Limit:                               1000
```

show track

セキュリティレベル合意（SLA）トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、**show track** コマンドを使用します。

show track ［*track-id*］

構文の説明

track-id	トラッキング エントリ オブジェクト ID 番号（1 ~ 500）。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、**show track** コマンドの出力例を示します。

```
> show track

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

show traffic

インターフェイスの送信アクティビティおよび受信アクティビティを表示するには、**show traffic** コマンドを使用します。

show traffic

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show traffic コマンドは、**show traffic** コマンドが最後に入力された時点またはデバイスがオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、デバイスが直前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

統計情報は、インターフェイス名に基づいて最初に表示されます。名前付きインターフェイスの後に、物理インターフェイスに基づいて統計情報が表示されます。インターフェイスには、システムが内部通信に使用する非表示の仮想インターフェイスが含まれることがあります。

例

次に、単体のインターフェイスの統計情報を示す**show traffic**コマンドの省略された出力例を示します。各インターフェイスは同じ統計情報を表示します。

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

関連コマンド

Command	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。

show upgrade

システムソフトウェアのアップグレードに関する情報を表示するには、**show upgrade** コマンドを使用します。

show upgrade { **revert-info** | **status** [**detail**] [**continuous**] }

構文の説明

revert-info	使用可能なバージョンがある場合は、復元して使用できるシステムのバージョンを表示します。使用可能な復元バージョンがない場合は、**upgrade revert** コマンドを使用できません。
status	アップグレードのステータスを表示します。次のオプションキーワードを含めることができます。 • **detail** ステータス情報の概要に加えて、アップグレードログを表示します。 • **continuous** 生成されたアップグレードメッセージを表示します。このキーワードは単独で使用することもできますが、detail キーワードと組み合わせて使用することもできます。

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。

使用上のガイドライン

ステータスには以下が含まれることがあります。

- 進行中のアップグレードはありません。
- メジャーアップグレードが進行中です。
- パッチアップグレードが進行中です。
- ホットフィックス アップグレードが進行中です。
- メジャーアップグレードに失敗しました。「cancel」を実行して回復します。

  リブートは、アップグレード失敗の段階によって発生する場合と発生しない場合があります。
- メジャーアップグレードに失敗しました。デバイスをリブートして回復します。

例

次の例は、現在進行中のアップグレードのステータスを示しています。完了したアップグレードのステータスを表示するには、**show last-upgrade status** コマンドを使用します。

```
> show upgrade status
Upgrade from 6.3.0 to 6.7.0 in progress (11% progress, time remaining 8 mins)
Time started: Tue Dec  3 23:50:31 UTC 2020
Current state: Tue Dec  3 23:51:01 UTC 2020 Running script 200_pre/001_check_reg.pl...
```

次の例は、復元に関する情報を示しています。この例では、復元できるバージョンが存在します。使用可能なバージョンがない場合、「No version is available for revert」というメッセージが表示されます。

```
> show upgrade revert-info
You can revert to version 6.4.0-102
at 2020-03-20T22:49:43+0000

It uses 4946MB of disk space.

Version 6.4.0-102 is available for revert.
```

関連コマンド

Command	説明
show last-upgrade status	最後のシステム ソフトウェア アップグレードに関する情報を表示します。
upgrade	システム ソフトウェア アップグレードをキャンセル、復元、または再試行します。

show user

デバイスのコマンドラインインターフェイス（CLI）にアクセスするためのユーザーアカウントを表示するには、**show user** コマンドを使用します。

show user ［*username1* ［*usernam2*］［...］］

構文の説明

username1 [*usernam2*] [...]	（オプション）1 つ以上のスペースで区切られたユーザー名。名前を指定しない場合は、すべてのユーザーが表示されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ユーザーごとに次の情報が表示されます。**configure user add** コマンドを使用してユーザーアカウントを作成します。

- Login：ログイン名。
- UID：ユーザー ID（数字）。
- Auth：ユーザーの認証方法。Local と Remote（ディレクトリサーバー経由）のいずれか。
- Access：ユーザーの権限レベル。Basic と Config のいずれか。この設定を変更するには、**configure user access** コマンドを使用します。
- Enabled：ユーザーがアクティブかどうか。Enabled と Disabled のいずれか。この設定を変更するには、**configure user enable**/**disable** コマンドを使用します。
- Reset：ユーザーが次回ログイン時にアカウントパスワードを変更する必要があるかどうか。Yes と No のいずれか。この設定を変更するには、**configure user forcereset** コマンドを使用します。
- Exp：ユーザーのパスワード変更が必要になるまでの日数。Never は、パスワードが期限切れにならないことを示します。この設定を変更するには、**configure user aging** コマンドを使用します。
- Warn：パスワードの有効期限が切れる前に、ユーザーがパスワードの変更を警告される日数。N/A は、警告が適用されないことを示します。この設定を変更するには、**configure user aging** コマンドを使用します。
- Grace：猶予期間。期限が切れた後にユーザーがパスワードを変更できる日数です。Disabled は猶予期間がないことを意味します。猶予期間は、FXOS を実行しているデバイスにのみ適用されます。この設定を変更するには、**configure user aging** コマンドを使用します。
- Str：ユーザーのパスワードが強度チェックの基準を満たす必要があるかどうか。Dis（無効）と Ena（有効）のいずれか。このオプションを設定するには、**configure user strengthcheck** コマンドを使用します。

- Lock：ログインの失敗が多すぎた場合に、ユーザーのアカウントをロックするかどうか。ユーザーアカウントのロックを解除するには、**configure user unlock** コマンドを使用します。
- Max：ユーザーのアカウントがロックされる前に許容されるログイン失敗の最大回数。N/A は、アカウントをロックできないことを示します。この設定を変更するには、configure user maxfailedlogins コマンドを使用します。

例

次に、CLI アクセス用に定義されたユーザーを表示する例を示します。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

次に、外部ユーザーと猶予期間を含める例を示します。

```
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No
5
```

関連コマンド

Command	説明
configure user add	CLI アクセス用のユーザーアカウントを追加します。

show version

ハードウェアモデル、ソフトウェアバージョン、UUID、侵入ルール更新バージョン、および VDB バージョンを表示するには、**show version** コマンドを使用します。

show version ［**detail** | **system**］

構文の説明

detail	**show version** と **show version detail** は同じ情報を表示します。
system	このキーワードは、**show version** によって表示される情報に付加的なシステム情報を追加します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.1	システムの起動（ブート）にかかった時間に関する情報が出力に追加されました。

使用上のガイドライン

show version コマンドと **show version detail** コマンドは、同じ基本的なシステム情報を表示します。**show version system** コマンドは、この情報に加えて、最後のリブート以降の動作時間やより具体的なハードウェア情報などの付加的なシステム情報を表示します。

例

次の例は、基本的な **show version** の出力を示しています。

```
> show version
-------------------[ firepower ]---------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.2.0 (Build 1405)
UUID : 78ddf634-3754-11ec-87dd-ace5f9ec4cdc
Rules update version : 2022-01-11-001-vrt
LSP version : lsp-rel-20220111-1030
VDB version : 348
-----------------------------------------------------
```

show version system コマンドの次の出力例では、**show version** コマンドと同じ出力に付加的な情報が追加されています。

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build
226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
-----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72
```

```
Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 36 days 21 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type                : Release
Key Version               : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

バージョン 7.1 以降では、システムの起動にかかった時間を確認できます。この情報は、システムの稼働時間のステータスの後に表示されます。

```
> show version system
---------------------[ ftdv1 ]----------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.1.0
 (Build 1519)
UUID                       : b964ed5e-92c0-11eb-aaa2-cfab359c2436
LSP version                : lsp-rel-20210310-2255
VDB version                : 338
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 99.17(1)135
SSP Operating System Version 82.11(1.277i)

Compiled on Thu 25-Mar-21 00:49 GMT by builders
System image file is "boot:/asa99171-135-smp-k8.bin"
Config file at boot was "startup-config"

ftdv1 up 6 days 22 hours
Start-up time 5 secs

(remaining output redacted)
```

show vlan

脅威に対する防御 デバイスに設定されているすべての VLAN を表示するには、**show vlan** コマンドを使用します。

show vlan ［**mapping** ［*primary_id*］］

構文の説明

mapping	（オプション）プライマリ VLAN にマッピングされたセカンダリ VLAN を表示します。
primary_id	（オプション）特定のプライマリ VLAN のセカンダリ VLAN を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、設定されている VLAN を表示する例を示します。

```
> show vlan
10-11,30,40,300
```

次に、各プライマリ VLAN にマッピングされたセカンダリ VLAN を表示する例を示します。

```
> show vlan mapping
Interface                       Secondary VLAN ID                       Mapped VLAN
ID
0/1.100                         200                                             300
0/1.100                         201                                             300
0/2.500                         400                                             200
```

関連コマンド

Command	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
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 vm

Threat Defense Virtual デバイス上の仮想プラットフォーム情報を表示するには、**show vm** コマンドを使用します。

show vm

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、VMware についての情報を表示する例を示します。

```
> show vm

Virtual Platform Resource Status
--------------------------------
Number of vCPUs           :  4
Processor Memory          :  8192 MB
Hypervisor                :  VMware
```

show vpdn

PPPoE または L2TP のような仮想プライベート ダイヤルアップ ネットワーク（VPDN）接続のステータスを表示するには、**show vpdn** コマンドを使用します。

show vpdn {**group** *name* | **pppinterface id** *number* | **session** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **window**} | **tunnel** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **summary** | **transport**} | **username** *name*}

構文の説明

group *name*	VPDN グループのコンフィギュレーションを表示します。
id *number*	（オプション）指定された ID を持つ VPDN セッションに関する情報を表示します。
l2tp	（オプション）L2TP に関するセッションまたはトンネルの情報を表示します。
packets	セッションまたはトンネル パケットの情報を表示します。
pppinterface	PPP インターフェイス情報を表示します。
pppoe	（オプション）PPPoE に関するセッションまたはトンネルの情報を表示します。
session	セッション情報を表示します。
state	セッションまたはトンネルの状態の情報を表示します。
summary	トンネルの概要を表示します。
transport	トンネルのトランスポート情報を表示します。
tunnel	トンネル情報を表示します。
username *name*	ユーザー情報を表示します。
window	セッション ウィンドウ情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

VPDN PPPoE 接続または L2TP 接続をトラブルシューティングするには、このコマンドを使用します。

例

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

```
> show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

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

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
```

show vpn load-balancing

このコマンドは使用しないでください。脅威に対する防御でサポートされていない機能に関連しています。

show vpn-sessiondb

VPNセッションに関する情報を表示するには、いずれかの**show vpn-sessiondb**コマンドを使用します。

show vpn-sessiondb ［**detail**］［**full**］｛**anyconnect** | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec**｝［**filter** *criteria*］［**sort** *criteria*］
show vpn-sessiondb ［**detail**］［**full**］ **index** *index-number*
show vpn-sessiondb failover
show vpn-sessiondb ospfv3 ［**filter ipaddress** *IP_address*］［**sort ipaddress**］

構文の説明

anyconnect	AnyConnect VPN クライアントセッションを表示します。
detail	（任意）セッションに関する詳細情報を表示します。たとえば、IPsecセッションに対して detail オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの詳細情報が表示されます。 detail および full オプションを指定すると、脅威に対する防御 デバイスはマシンで読み取り可能な形式で詳細な出力を表示します。
failover	フェールオーバー IPSec トンネルのセッション情報を表示します。
filter *filter_criteria*	（任意）指定したフィルタオプションに従って、出力をフィルタ処理します。オプションのリストについては、「使用上のガイドライン」を参照してください。
full	（任意）連続した、短縮されていない出力を表示します。出力のレコード間には | 文字と || ストリングが表示されます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号を指定します。範囲は 1 ～ 65535 です。
l2l	VPN の LAN-to-LAN セッション情報を表示します。
ospfv3	OSPFv3 セッション情報を表示します。
ra-ikev1-ipsec	IPsec IKEv1 セッションを表示します。
ra-ikev2-ipsec	IKEv2 リモート アクセス クライアント接続の詳細を表示します。
sort *sort_criteria*	（任意）指定するソート オプションに従って出力をソートします。オプションのリストについては、「使用上のガイドライン」を参照してください。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

次のオプションを使用して、セッションに関する表示内容をフィルタ処理およびソートできます。フィルタ処理およびソートできる値は、リストするセッションタイプによって異なります。

フィルタ/ソート オプション	説明
filter a-ipaddress *IP_address*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）に関する情報だけを表示します。 次と併用：**anyconnect**、**ra-ikev2-ipsec**
sort a-ipaddress	割り当て済み IP アドレスで表示内容をソートします。 次と併用：**anyconnect**、**ra-ikev2-ipsec**
filter a-ipversion {**v4** | **v6**}	IPv4 または IPv6 アドレスが割り当てられたセッションのみを表示するように出力をフィルタ処理します。 使用対象：**anyconnect**、**ra-ikev2-ipsec**
filter encryption *encryption_algorithm*	出力をフィルタ処理して、指定した暗号化アルゴリズムを使用しているセッションに関する情報のみを表示します。使用可能なメソッドを確認するには、**?** を使用します。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**
sort encryption	セッションで使用される暗号化アルゴリズムで出力をソートします。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**
filter inactive	アイドル状態であり、（ハイバネーション、モバイルデバイス切断などによって）接続が切断された可能性がある非アクティブなセッションをフィルタ処理します。TCP キープアライブが AnyConnect クライアントからの応答なしで 脅威に対する防御 デバイスから送信されると、非アクティブなセッションの数が増加します。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションが SSL トンネルを介してアクティブにトラフィックを渡している場合、00:00m:00s が表示されます。 次と併用： **anyconnect** （注） 脅威に対する防御 デバイスは、バッテリ寿命を節約するために一部のデバイス（iPhone、iPad、iPod など）に TCP キープアライブを送信しないため、障害検出で切断とスリープが区別されません。そのため、非アクティブなカウンタは設計によって 00:00:00 のままになります。
sort inactivity	非アクティブなセッションでソートします。 次と併用： **anyconnect**

フィルタ/ソート オプション	説明
filter ipaddress *IP_address*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）に関する情報だけを表示します。 次と併用：**l2l**、**ospfv3**
sort ipaddress	内部 IP アドレスで表示内容をソートします。 次と併用：**l2l**、**ospfv3**
filter ipversion {**v4** | **v6**}	出力をフィルタ処理して、IPv4 または IPv6 アドレスを割り当てられたエンドポイントから開始されるセッションのみを表示します。 次と併用： **l2l**
filter name *username*	出力をフィルタ処理して、指定したユーザー名のセッションを表示します。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**
sort name	ユーザー名のアルファベット順に表示内容をソートします。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**
filter p-ipaddress *IP_address*	出力をフィルタ処理して、指定したパブリック外部 IP アドレスに関する情報のみを表示します。 次と併用：**anyconnect**、**ra-ikev2-ipsec**
sort p-ipaddress	パブリック外部 IPアドレスで表示内容をソートします。 次と併用：**anyconnect**、**ra-ikev2-ipsec**
filter p-ipversion {**v4** | **v6**}	出力をフィルタ処理して、パブリック IPv4 または IPv6 アドレスを割り当てられたエンドポイントから開始されるセッションのみを表示します。 次と併用：**anyconnect**、**ra-ikev2-ipsec**
filter protocol *name*	出力をフィルタ処理して、指定したプロトコルを使用しているセッションに関する情報のみを表示します。使用可能なプロトコルを確認するには、**?** を使用します。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**
sort protocol	プロトコルで表示内容をソートします。 次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec**

次の表で、出力に表示される可能性のあるフィールドについて説明します。

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

フィールド	説明
IKE Sessions	IKE（IPsec フェーズ 1）セッションの数で、通常は 1。これらのセッションにより、IPsec トラフィックのトンネルが確立されます。
索引	このレコードの固有識別情報。
IP Addr	このセッションのリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。
IPsec Sessions	IPsec（フェーズ 2）セッション（トンネル経由のデータ トラフィック セッション）の数。各 IPsec リモート アクセス セッションには、2 つの IPsec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
ライセンス情報	共有 SSL VPN ライセンスに関する情報を表示します。
Local IP Addr	トンネルのローカルエンドポイント（システム上のインターフェイス）に割り当てられた IP アドレス。
Login Time	セッションにログインした日時（MMM DD HH:MM:SS）。時刻は 24 時間表記で表示されます。
NAC Result	ネットワーク アドミッション コントロール ポスチャ検証の状態。次のいずれかを指定できます。 • [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。 • [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。 • [Exempted]：脅威に対する防御 デバイスに設定されたポスチャ検証免除リストに従って、リモートホストはポスチャの検証を免除されています。 • [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。 • [Hold-off]：ポスチャ検証に成功した後、脅威に対する防御 デバイスとリモートホストの EAPoUDP 通信が切断されました。 • [N/A]：VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。 • [Unknown]：ポスチャ検証が進行中です。

フィールド	説明
NAC Sessions	ネットワーク アドミッション コントロール（EAPoUDP）セッションの数。
Packets Rx	システムがリモートピアから受信したパケット数。
Packets Tx	システムがリモートピアに送信したパケット数。
PFS Group	完全転送秘密グループ番号。
Posture Token	Access Control Server 上で設定可能な情報テキスト ストリング。ACS は、情報提供のためにシステムにポスチャトークンをダウンロードして、システムモニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。
リダイレクト URL	ポスチャ検証またはクライアントレス認証に続いて、ACS はセッションのアクセスポリシーをシステムにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。システムは、リモートホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセスポリシーに Redirect URL が含まれていない場合、脅威に対する防御 デバイスはリモートホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。 Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。
Rekey Int（T または D）	IPsec（IKE）SA 暗号キーの有効期限。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。
Rekey Left（T または D）	IPsec（IKE）SA 暗号キーの残りのライフタイム。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。
Rekey Time Interval	IPsec（IKE）SA 暗号キーの有効期限。
Remote IP Addr	トンネルのリモートエンドポイント（リモートピア上のインターフェイス）に割り当てられた IP アドレス。

フィールド	説明
Reval Int (T)	Revalidation Time Interval。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Reval Left (T)	Time Until Next Revalidation。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Session ID	セッション コンポーネント（サブセッション）の ID。各 SA には独自の ID があります。
Session Type	セッションのタイプ（LAN-to-LAN または Remote）。
SQ Int (T)	Status Query Time Interval。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータスクエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、システムがリモートホストに発行する要求です。
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータスクエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、システムがリモートホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Tunnel Group	属性値を求めるために、このトンネルが参照するトンネル グループの名前。
UDP Dst Port または UDP Destination Port	リモート ピアが使用する UDP のポート番号。
UDP Src Port または UDP Source Port	UDP 用に使用されるポート番号。
Username	セッションを確立したユーザーのログイン名。

フィールド	説明
VLAN	このセッションに割り当てられた出力 VLAN インターフェイス。システムは、すべてのトラフィックをこのVLANに転送します。グループポリシーまたは継承されたグループポリシーのいずれかによって値が指定されます。

例

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

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1            Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :         42
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
------------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
--------------------------------------------------------------------------------
```

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

```
> show vpn-sessiondb detail
--------------------------------------------------------------------------------
```

```
VPN Session Summary
------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
------------------------------------------------------------------------------

------------------------------------------------------------------------------
Tunnels Summary
------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
------------------------------------------------------------------------------
Totals                      :      3 :         42
------------------------------------------------------------------------------
```

次に、**show vpn-sessiondb detail l2l** コマンドの出力例を示します。

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
Remote Addr : 209.165.201.30/255.255.255.0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel PFS Group : 5
Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
```

```
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 240 Bytes Rx : 160
Pkts Tx : 3 Pkts Rx : 2

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb detail index 1** コマンドの出力例を示します。

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

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

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

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

次に、**show vpn-sessiondb ospfv3** コマンドの出力例を示します。

```
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

次に、**show vpn-sessiondb detail ospfv3** コマンドの出力例を示します。

```
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 105268 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb detail anyconnect** コマンドの出力例を示します。

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab Index : 2
Assigned IP : 65.2.1.100 Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx : 0 Bytes Rx : 21248
Pkts Tx : 0 Pkts Rx : 238
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : test1
Login Time : 22:44:59 EST Tue Aug 13 2017
```

```
Duration : 0h:02m:42s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 75.2.1.60
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 400 Minutes Idle TO Left : 397 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : 3.1.05050

IKEv2:
Tunnel ID : 2.2
UDP Src Port : 64251 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86241 Seconds
PRF : SHA1 D/H Group : 2
Filter Name : mixed1
Client OS : Windows

IPsecOverNatT:
Tunnel ID : 2.3
Local Addr : 75.2.1.23/255.255.255.255/47/0
Remote Addr : 75.2.1.60/255.255.255.255/47/0
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport, GRE
Rekey Int (T): 28400 Seconds Rekey Left(T): 28241 Seconds
Idle Time Out: 400 Minutes Idle TO Left : 400 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Bytes Tx : 0 Bytes Rx : 21326
Pkts Tx : 0 Pkts Rx : 239

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 165 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb ra-ikev2-ipsec** コマンドの出力例を示します。

```
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 17844
```

```
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

次に、**show vpn-sessiondb anyconnect** コマンドの出力例を示します。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                  Index        : 19576
Assigned IP  : 192.168.3.243          Public IP    : 192.168.10.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel:
(1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15060                  Bytes Rx     : 20631
Group Policy : DfltGrpPolicy          Tunnel Group : Ad_group
Login Time   : 09:24:53 UTC Fri Apr 7 2017
Duration     : 0h:03m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none                   Tunnel Zone  : 0
```

関連コマンド

コマンド	説明
clear vpn-sessiondb statistics	VPN セッション統計をクリアします。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。
show vpn-sessiondb summary	現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、**show vpn-sessiondb ratio** コマンドを使用します。

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

構文の説明

encryption	各暗号化方式を使用しているセッションの数とセッションの割合を表示します。
protocol	各 VPN プロトコルを使用しているセッションの数とセッションの割合を表示します。
filter *groupname*	（オプション）出力をフィルタリングして、指定するトンネルグループについてのみセッションの比率を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、暗号化に基づくセッションの比率を表示する例を示します。

```
> show vpn-sessiondb ratio encryption

Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Tunnels        Percent
none                     0                0%
DES                      0                0%
3DES                     0                0%
RC4                      0                0%
AES128                   4               80%
AES192                   1               20%
AES256                   0                0%
AES-GCM-128              0                0%
AES-GCM-192              0                0%
AES-GCM-256              0                0%
AES-GMAC-128             0                0%
AES-GMAC-192             0                0%
AES-GMAC-256             0                0%
```

次に、プロトコルに基づくセッションの比率を表示する例を示します。

```
> show vpn-sessiondb ratio protocol

Filter Group         : All
Total Active Tunnels : 3
Cumulative Tunnels   : 42
```

```
Protocol                Tunnels         Percent
IKEv1                   0                 0%
IKEv2                   0                 0%
IPsec                   0                 0%
IPsecLAN2LAN            0                 0%
IPsecLAN2LANOverNatT    0                 0%
IPsecOverNatT           0                 0%
IPsecOverTCP            0                 0%
IPsecOverUDP            0                 0%
L2TPOverIPsec           0                 0%
L2TPOverIPsecOverNatT   0                 0%
Clientless              0                 0%
Port-Forwarding         0                 0%
IMAP4S                  0                 0%
POP3S                   0                 0%
SMTPS                   0                 0%
AnyConnect-Parent       1                33%
SSL-Tunnel              1                33%
DTLS-Tunnel             1                33%
```

関連コマンド

コマンド	説明
show vpn-sessiondb	VPN セッションに関する情報を表示します。
show vpn-sessiondb summary	現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。

show vpn-sessiondb summary

アクティブセッションの数の概要を表示するには、**show vpn-sessiondb summary** コマンドを使用します。

show vpn-sessiondb summary

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

次の表に、Active Sessions サマリーおよび Session Information サマリーに含まれるフィールドの説明を示します。

フィールド	説明
Concurrent Limit	このシステムで許可された、同時にアクティブにできるセッションの最大数。
Cumulative Sessions	システムが最後に起動またはリセットされたとき以降の全タイプのセッション数。
LAN-to-LAN	現在アクティブな IPsec LAN-to-LAN セッションの数。
Peak Concurrent	システムが最後に起動またはリセットされたとき以降に同時にアクティブだった、全タイプのセッションの最大数。
Percent Session Load	使用中の VPN セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。
リモートアクセス	ra-ikev1-ipsec：現在アクティブな IKEv1 IPsec リモートアクセスユーザー、L2TP over IPsec、および IPsec through NAT セッションの数。
Total Active Sessions	現在アクティブな全タイプのセッションの数。

例

次に、**show vpn-sessiondb summary** コマンドの出力例を示します。

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-----------------------------------------
OSPFv3 IPsec : 1 : 1 : 1
-------------------------------------------------------------------------
```

```
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
--------------------------------------------------------------------------
```

次に、一般的な IKEv2 IPsec リモートアクセスセッションに関する **show vpn-sessiondb summary** コマンドの出力例を示します。

```
> show vpn-sessiondb summary
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
Generic IKEv2 Remote Access : 1 : 1 : 1
--------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%
--------------------------------------------------------------------------

--------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
----------------------------------------------
IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1
--------------------------------------------------------------------------
Totals : 2 : 2
--------------------------------------------------------------------------
```

関連コマンド

コマンド	説明
show vpn-sessiondb	VPN セッションに関する情報を表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show vrf

システムで定義されている仮想ルータの情報を表示するには、**show vrf** コマンドを使用します。

show vrf ［**counters** | **lock**］

構文の説明

counters	（任意）このシステムで許可されるユーザー定義の仮想ルータの最大数と、設定されている実際の仮想ルータの数を表示します。最大数 doc にはグローバル仮想ルータは含まれません。たとえば、最大数が 4 の場合、上限の合計は 5 となります。
lock	（任意）VRF ロック情報を表示します。

コマンド デフォルト

キーワードを指定しないと、現在の仮想ルータと各仮想ルータに割り当てられているインターフェイスが表示されます。

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

Virtual Route Forwarding（VRF）を有効にした場合は、**show vrf** コマンドを使用して、システムで定義された仮想ルータに関する基本情報を表示します。各仮想ルータのルーティングテーブルを表示するには、IPv4 ルーティングテーブルでは **show route vrf** *name* コマンドを使用し、IPv6 ルーティングテーブルでは **show ipv6 route vrf** *name* を使用します。

例

次に、仮想ルータと各ルータに割り当てられたインターフェイスを表示する例を示します。

```
> show vrf

Name            VRF ID          Description             Interfaces
vrf1            1                                       inside
                                                        inside_2
vrf2            2                                       inside_3
                                                        inside_4
```

次の例は、このシステムで許可される仮想ルータの最大数と、仮想ルータの現在の数を示しています。仮想ルータが IPv4、IPv6、またはその両方であるかどうかは、各仮想ルータ内のインターフェイスに割り当てる IP アドレスによって異なります。最大数はユーザー定義の仮想ルータを指すことに注意してください。この例では、VMware システムの場合、許容される上限の合計は 15 です（グローバル仮想ルータが 1 つ、ユーザー定義ルータが 14）。

```
> show vrf counters
Maximum number of VRFs supported: 14
Maximum number of IPv4 VRFs supported: 14
Maximum number of IPv6 VRFs supported: 14
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

次に、VRF ロック情報の例を示します。

```
> show vrf lock

VRF Name: single_vf; VRF id = 0 (0x0)
VRF lock count: 1
VRF Name: vrf1; VRF id = 1 (0x1)
VRF lock count: 2
VRF Name: vrf2; VRF id = 2 (0x2)
VRF lock count: 2
```

関連コマンド

Command	説明
show ipv6 route	IPv6 ルーティングテーブルを表示します。
show route	IPv4 ルーティングテーブルを表示します。

show wccp

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

show wccp {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]
show wccp [**interfaces** [**detail**]]

構文の説明

buckets	（オプション）サービスグループのバケット割り当て情報を表示します。
detail	（任意）ルータおよびすべての Web キャッシュに関する情報を表示します。
hash *dest_addr source_addr dest_port source_port*	（オプション）指定された接続の WCCP ハッシュを表示します。 • *dest_addr* は宛先ホストの IP アドレスです。 • *source_addr* は送信元ホストの IP アドレスです。 • *dest_port* は宛先ホストのポートです。 • *source_port* は送信元ホストのポートです。
interfaces [**detail**]	（オプション）WCCP リダイレクトインターフェイスを表示します。インターフェイス コンフィギュレーションの detail キーワードが含まれます。
service	（オプション）サービスグループの定義情報を表示します。
service-number	キャッシュが制御する Web キャッシュサービスグループの ID 番号。番号は、0 ～ 254 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。
view	（オプション）特定のサービスグループの他のメンバーが検出されたかどうかを表示します。
web-cache	Web キャッシュ サービスの統計情報を指定します。

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

例

次に、WCCP 情報を表示する例を示します。

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

関連コマンド

コマンド	説明
clear wccp	WCCP 統計情報をクリアします。

show webvpn

リモートアクセス VPN に関する情報を表示するには、**show webvpn** コマンドを使用します。

show webvpn {**anyconnect** | **debug-condition** | **group-alias** [*tunnel_group*] | **group-url** [*tunnel_group*] | **statistics**}

構文の説明

anyconnect	クライアントエンドポイントにダウンロード可能なAnyConnectイメージに関する情報を表示します。
debug-condition	**debug webvpn condition** コマンドによって設定されている現在のデバッグ条件を表示します。
group-alias [*tunnel_group*]	トンネルグループ（接続プロファイル）のエイリアスを表示します。オプションとして、トンネルグループの名前を指定し、指定したグループに関する情報のみを表示することもできます。各グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。
group-url [*tunnel_group*]	トンネルグループ（接続プロファイル）の URL を表示します。オプションとして、トンネルグループの名前を指定し、指定したグループに関する情報のみを表示することもできます。各グループには複数の URL があることも、URL がまったくないこともあります。
statistics	WebVPN イベントに関するデータを表示します。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。
7.1	外部ブラウザパケットに関する情報が AnyConnect の出力に追加されました。

例

show webvpn anyconnect コマンドの出力例を次に示します。

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
  CISCO STC win2k+
  4,2,06014
  Hostscan Version 4.2.06014
  Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

次に、SAML 認証で使用されている場合は、外部ブラウザパッケージが含まれている **show webvpn anyconnect** の例を示します。

```
> show webvpn anyconnect
1. disk0:/anyconnpkgs/anyconnect-win-4.10.01075-webdeploy-k9.pkg 2 dyn-regex=/Windows
NT/
  CISCO STC win2k+
  4,10,01075
  Hostscan Version 4.10.01075
  Wed 04/28/2021 12:36:03.98

1 AnyConnect Client(s) installed

2. disk0:/externalbrowserpkgs/external-sso-98.161.00015-webdeploy-k9.pkg
  Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 05/05/21 15:49:27.817381
```

show webvpn debug-condition コマンドの出力例を次に示します。

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

show webvpn group-alias コマンドの出力例を次に示します。

```
> show webvpn group-alias
Tunnel Group: Ad_group   Group Alias: ad_group enabled
Tunnel Group: Radius_group   Group Alias: Radius_group enabled
Tunnel Group: Cert_auth   Group Alias: cert_auth enabled
```

show webvpn group-url コマンドの出力例を次に示します。

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

show webvpn statistics コマンドの出力例を次に示します。

```
> show webvpn statistics
Total number of objects served  0
 html                           0
 js                             0
 css                            0
 vb                             0
 java archive                   0
 java class                     0
 image                          0
 undetermined                   0
Server compression statistics
 Decompression success from server                  0
 Unsolicited compression from server                0
 Unsupported compression algorithm used by server   0
 Decompression failure for server responses         0
IOBuf failure statistics
```

```
uib_create_with_channel                          0
uib_create_with_string                           0
uib_create_with_string_and_channel               0
uib_transfer                                     0
uib_add_filter                                   0
uib_yyread                                       0
uib_read                                         0
uib_set_buffer_max                               0
uib_set_eof_symbol                               0
uib_get_capture_handle                           0
uib_set_capture_handle                           0
uib_buflen                                       0
uib_bufptr                                       0
uib_buf_endptr                                   0
uib_get_buf_offset                               0
uib_get_buf_offset_addr                          0
uib_get_nth_char                                 0
uib_consume                                      0
uib_advance_bufptr                               0
uib_eof                                          0
```

show xlate

NAT セッション（xlates または変換）の情報を表示するには、**show xlate** コマンドを使用します。

show xlate ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］
show xlate count

構文の説明

count	変換数を表示します。
global *ip1*[*-ip2*]	（任意）アクティブな変換をマッピングされた IP アドレスまたはアドレスの範囲別に表示します。
gport *port1*[*-port2*]	（任意）アクティブな変換をマッピングされたポートまたはポートの範囲別に表示します。
interface *if_name*	（任意）アクティブな変換をインターフェイス別に表示します。
local *ip1*[*-ip2*]	（任意）アクティブな変換を実際の IP アドレスまたはアドレスの範囲別に表示します。
lport *port1*[*-port2*]	（任意）アクティブな変換を実際のポートまたはポートの範囲別に表示します。
netmask *mask*	（任意）マッピングされた、または実際の IP アドレスを限定するネットワーク マスクを指定します。
type *type*	（任意）アクティブな変換をタイプ別に表示します。次のタイプを 1 つ以上入力できます。 • **static** • **portmap** • **dynamic** • **twice-nat**（別名、手動 NAT） 複数のタイプを指定する場合は、タイプをカンマで区切ります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show xlate コマンドは、変換スロットの内容を表示します。xlate には、デバイスマネージャの NAT ルールテーブルに表示されない、内部インターフェイス用に生成されたものを含めることができます。これらは内部処理に必要です。

VPN クライアント コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合に **show xlate** コマンドを実行すると、1 つのスタティック変換に対応する複数の xlate が表示されることがあります。

クラスタリング環境では、PAT セッションを処理するために、最大 3 つの xlate が、クラスタ内の異なるノードに複製される可能性があります。1 つの xlate は、接続を所有するユニットで作成されます。1 つの xlate は、PAT アドレスをバックアップするために別のユニットで作成されます。最後の 1 つの xlate は、フローを複製するディレクタにあります。バックアップとディレクタが同じユニットである場合、3 つではなく 2 つの xlate が作成されることがあります。

例

次に、**show xlate** コマンドの出力例を示します。nlp_int_tap の初期 PAT xlate は、Device Manager が管理インターフェイスアドレスではなく 192.168.1.1 にアクセスできるようにする HTTPS アクセスルールに関連しています。これらは、デバイスマネージャの NAT テーブルにルールが表示されない内部 NAT xlate です。

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

次に、IPv4 から IPv6 への変換を示す **show xlate** コマンドの出力例を示します。

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
```

```
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

関連コマンド

Command	説明
clear xlate	現在の変換および接続情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。

show zone

トラフィックゾーン情報を表示するには、**show zone** コマンドを使用します。

show zone ［*name*］

構文の説明

name	（オプション）トラフィックゾーンの名前。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

トラフィックゾーンは、セキュリティゾーンとまったく同じではありません。パッシブセキュリティゾーンもトラフィックゾーンとして自動的に生成されますが、ルーテッドおよびスイッチ ドセキュリティ ゾーンは生成されません。トラフィックゾーンは、トラフィックのロードバランシング（等コストマルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングのために使用できます。

ゾーン設定の残りの部分を表示するには、**show running-config zone** および **show running-config interface** コマンドを使用します。

例

次に、設定されたトラフィックゾーンを表示する例を示します。この例では、トラフィックゾーンはパッシブインターフェイス用です。等コストマルチパスルーティングのゾーンの場合、ゾーンタイプは ecmp になります。インターフェイスの設定は次のとおりです。**zone-member** コマンドは、インターフェイスをゾーンのメンバーとして設定します。

```
> show zone passive-security-zone
Zone: passive-security-zone passive
    Security-level: 0
    Zone member(s): 1
      passive                       GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 mode passive
 nameif passive
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 zone-member krjones-passive-security-zone
```

関連コマンド

Command	説明
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
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 local-host zone	ゾーン内のローカル ホストのネットワーク状態を表示します。
show nameif zone	インターフェイスのゾーンまたはインライン セット メンバーシップを表示します。

shun

攻撃元ホストからの接続をブロックするには、**shun** コマンドを使用します。shun を無効にするには、このコマンドの **no** 形式を使用します。

shun *source_ip* ［*dest_ip source_port dest_port* ［*protocol*］］［**vlan** *vlan_id*］
no shun *source_ip* ［**vlan** *vlan_id*］

構文の説明

dest_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。
dest_ip	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。
protocol	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。
source_ip	攻撃元ホストのアドレスを指定します。送信元 IP アドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。
source_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。
vlan *vlan_id*	（任意）送信元ホストが配置されている VLAN ID を指定します。

コマンド デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続をブロックできます。該当する送信元 IP アドレスからの今後の接続すべては、手動でブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。**shun** コマンドのブロッキング機能は、指定したホストアドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

shun コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

shun コマンドは攻撃をダイナミックにブロックするために使用されるため、脅威に対する防御 デバイス コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。

例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、脅威に対する防御デバイスの接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、**shun** コマンドを適用します。

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

このコマンドにより、現在の接続が脅威に対する防御デバイスの接続テーブルから削除され、10.1.1.27からの今後のすべてのパケットは脅威に対する防御デバイスを通過できなくなります。

関連コマンド

Command	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
show conn	すべてのアクティブな接続を表示します。
show shun	回避についての情報を表示します。

shutdown

デバイスをシャットダウンするには、**shutdown** コマンドを使用します。

shutdown

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

例

次に、デバイスをシャットダウンしたときの**shutdown**コマンドの出力例を示します。

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

関連コマンド

Command	説明
reboot	デバイスをリブートします。

system access-control clear-rule-counts

アクセスコントロールルールのヒット数を 0 にリセットするには、**system access-control clear-rule-counts** コマンドを使用します。

system access-control clear-rule-counts

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

system access-control clear-rule-counts コマンドの出力例を次に示します。

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

関連コマンド

Command	説明
show access-control-config	nbr_router_id interface_name

system generate-troubleshoot

シスコテクニカルサポートで分析するためのトラブルシューティングデータの生成を要求された場合は、**system generate troubleshoot** コマンドを使用します。

system generate-troubleshoot *options*

構文の説明

オプション	生成するトラブルシューティングデータのタイプを表示します。1つ以上のオプションを入力できます。複数のオプションを区切るには、スペースを使用します。 • **ALL**：次のすべてのオプションを実行します。 • **SNT**：Snort のパフォーマンスと設定。 • **PER**：ハードウェアのパフォーマンスとログ。 • **SYS**：システム設定、ポリシー、およびログ。 • **DES**：検出設定、ポリシー、およびログ。 • **NET**：インターフェイスとネットワーク関連データ。 • **VDB**：検出、認知、VDB データ、およびログ。 • **UPG**：データとログのアップグレード。 • **DBO**：すべてのデータベースデータ。 • **LOG**：すべてのログデータ。 • **NMP**：ネットワークマップ情報。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、Snort およびハードウェアパフォーマンスのトラブルシューティング データを生成する例を示します。

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

関連コマンド

Command	説明
copy	システムとの間でファイルをコピーします。
delete	システムからファイルを削除します。

system lockdown-sensor

エキスパートモードおよび bash シェルへのアクセスを削除するには、**system lockdown-sensor** コマンドを使用します。

system lockdown-sensor

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

注意 このコマンドを実行すると元に戻すことはできません。エキスパートモードへのアクセスを復元する必要がある場合は、Cisco Technical Assistance Center に連絡して、ホットフィックスを入手する必要があります。

expert コマンドは、システムの動作環境への広範なアクセス権を管理者ユーザーに付与する bash シェルへのアクセスを提供します。セキュリティ認定方式（コモンクライテリア（CC）や Unified Capabilities Approved Products List（UC APL）など）では、システムのユーザーが利用できるアクセス権と情報を制限する要件が課されています。これらの認証要件を満たすための **expert** コマンドへのアクセスを削除するには、**system lockdown-sensor** コマンドを使用します。

（注） このコマンドを使用した後も、**expert** コマンドは現在の SSH セッションで引き続き使用できます。ログアウトしてから再度ログインし、このコマンドが削除されて機能しなくなったことを確認する必要があります。このコマンドを使用した後にログインした他のユーザーは、エキスパートモードも使用できません。

例

次の例では、セキュリティ要件に準拠するためにエキスパートモードへのアクセスを削除します。

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
>
```

system support コマンド

ほとんどの system support コマンドは、Cisco Technical Assistance Center のサポートを受けて、デバッグおよびトラブルシューティングを行うために使用されます。各コマンドはシスコサポートの指示に従い使用する必要があります。ただし、次のコマンドは一般的な目的で使用されます。

- system support diagnostic-cli （128 ページ）
- system support view-files （134 ページ）
- system support ssl-hw- コマンド （130 ページ）

system support ssl-client-hello- コマンド

これらのコマンドを使用すると、Transport Layer Security（TLS）1.3 から TLS 1.2 へのダウングレードの動作を決定できます。管理対象デバイスは TLS 1.3 暗号化または復号化をサポートしていないため、クライアントとサーバー間の TLS 1.3 セッションが中断し、クライアント Web ブラウザで次のようなエラーが発生する可能性があります。

ERR_SSL_PROTOCOL_ERROR

SEC_ERROR_BAD_SIGNATURE

ERR_SSL_VERSION_INTERFERENCE

クライアントがサーバーに接続し、ダウングレードするように変更された接続が [Do Not Decrypt SSL] ルールアクションと一致すると TLS インスペクションが判断した場合、エラーが発生する可能性があります。

これらのコマンドは、Cisco TAC に相談してから使用することを推奨します。

system support ssl-client-hello-enabled aggressive_tls13_downgrade { **true** | **false** }

構文の説明

true	これがデフォルトです。TLS 1.3 接続は、復号化の実行に必要な場合は常にダウングレードされます。ただし、ClientHello メッセージの後に受信したデータが原因でセッションが [Do Not Decrypt] ルールに一致した場合は、セッションが失敗する可能性があります。
false	TLS 1.3 接続は、セッションが [Do Not Decrypt] ルールに一致しない合理的な確実性がある場合にのみダウングレードされます。場合によっては、復号化が必要な TLS 接続がダウングレードされないことがあります。このような場合、トラフィックは復号化されません。代わりに、[Undecryptable Action] の [Session not cached] 設定の SSL ポリシーで指定されたアクションが実行されます。

コマンド履歴

リリース	変更内容
6.2.3.7	このコマンドが導入されました。

system support diagnostic-cli

追加の show コマンドやその他のトラブルシューティング コマンドを含む診断 CLI を開始するには、**system support diagnostic-cli** コマンドを使用します。

system support diagnostic-cli

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

診断 CLI には、システムのトラブルシューティングに使用できる追加の show コマンドやその他のコマンドが含まれています。診断CLIのコマンドは、ASA ソフトウェアのコマンドです。通常の 脅威に対する防御 CLI には同じコマンドが多数含まれているため、診断 CLI の追加コマンドは不要な場合があります。

診断 CLI を開始すると、通常の 脅威に対する防御 CLI とは別のセッションが開始されます。

プロンプトが変更され、システムのホスト名が表示されます。2 つのモードがあり、プロンプトに現在のモードが示されます。ユーザー EXEC モードの場合、プロンプトは次のとおりです。

```
hostname>
```

特権 EXEC モード（別名 Enable モード）の場合、プロンプトは次のようになります。このモードは、enable コマンドを使用して開始します。パスワードの入力を求められたら、Enter を押します。デフォルトでは、このモードを開始するためにパスワードを入力する必要はありません。

```
hostname#
```

診断 CLI を使用する場合は、次のヒントに留意してください。

- 診断 CLI を終了して通常の CLI に戻るには、Ctrl+a を押してから d を押します。
- 特権 EXEC モードを終了するには、**exit** コマンドを使用します。

  使用できるコマンドはモードによって異なります。特権EXECモードには、ユーザーEXECモードよりもはるかに多くのコマンドが含まれています。使用可能なコマンドを表示するには、**?**を使用します。ASA ソフトウェアのコマンドリファレンスで使用法の情報を確認できます。

  - Cisco ASA シリーズ コマンド リファレンス、A ～ H コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html
  - Cisco ASA シリーズ コマンド リファレンス、I ～ R コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html

  - Cisco ASA シリーズ コマンド リファレンス、S コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンド および ASASM 用 IOS コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- 診断 CLI には、脅威に対する防御 には意味のないコマンドが含まれていることがあります。コマンドを試しても意味のある（または何らかの）情報が表示されない場合、関連する機能が設定されていないか、または 脅威に対する防御 でサポートされていない可能性があります。
- 診断CLIでは、コンフィギュレーション モードを開始できません。CLIを使用してデバイスを設定することはできません。
- 診断CLIから離れると、次に診断CLIを開始した際には、最後に離れたときと同じモードになります。
- ASA 5506W-X では、**session wlan** コマンドを使用してワイヤレスモジュールへの接続を開き、そのCLIを使用してアクセスポイントを設定できます。この場合、特権EXECモードである必要があります。

例

次に、診断 CLI および特権 EXEC モードを開始する例を示します。**enable** コマンドの入力後にパスワードプロンプトが表示されたら、Enterを押します。デフォルトでは、特権 EXEC モードを開始するためのパスワードはありません。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

system support ssl-hw- コマンド

これらのコマンドを使用すると、バージョン 6.2.3 および 6.3 では *TLS/SSL* ハードウェア アクセラレーション、またバージョン 6.4 では *TLS* 暗号化アクセラレーション と呼ばれる機能に対してさまざまな操作を実行できます。使用可能なキーワードは、脅威に対する防御 ソフトウェアのバージョンによって異なります。

サポートされるデバイス、および機能がデフォルトで有効か無効かは、ソフトウェアバージョンによっても異なります。詳細については、『*Management Center CLI Configuration Guide*』を参照してください。

バージョン 6.2.3 および 6.3 のシンタックス：

system support {**ssl-hw-status** | **ssl-hw-supported-ciphers** | **ssl-hw-offload enable** | **ssl-hw-offload disable**}

バージョン 6.4 のシンタックス：

system support ssl-hw-supported-ciphers

構文の説明

ssl-hw-status	SSL ハードウェア アクセラレーションの現在のステータスを表示します。デフォルトの状態は次のとおりです。 • 6.2.3：無効 • 6.3 および 6.4：有効
ssl-hw-supported-ciphers	SSL ハードウェア アクセラレーションでサポートされている暗号のリストを表示します。このコマンドは、SSL ソフトウェア アクセラレーションでサポートされているすべての暗号を SSL ハードウェア アクセラレーションがサポートしているわけではないので便利です（特に、SEED 暗号と Camellia 暗号の暗号解読はサポートされていません）。
ssl-hw-offload enable	ハードウェア アクセラレーションを有効化します。デバイスを再起動するように求められます。
ssl-hw-offload disable	SSL ハードウェア アクセラレーションを無効化します。デバイスを再起動するように求められます。

コマンド履歴

リリース	変更内容
6.4	機能名が TLS/SSL ハードウェア アクセラレーション から TLS 暗号化アクセラレーション に変更されました。 次のキーワードが削除されました。 **ssl-hw-offload enable** **ssl-hw-offload disable** **ssl-hw-status**
6.3	この機能は、デフォルトでイネーブルに設定されています。
6.2.3	このコマンドが導入されました。この機能はデフォルトで無効に設定されています。

使用上のガイドライン

（注） このセクションで説明するコマンドのうち、バージョン 6.4 に適用されるのは **system support ssl-hw-offload-supported ciphers** のみです。

SSL ハードウェア アクセラレーションに関する情報を表示したり、機能を有効または無効にしたりするには、次のコマンドを使用します。

SSL ハードウェア アクセラレーションを有効にして、暗号化と暗号解読のパフォーマンスを向上させます。

サポートされていない機能を使用する場合、または SSL ポリシーを有効にした状態で予期しないトラフィックの中断が発生した場合は、SSL ハードウェア アクセラレーションを無効にします。

SSL ハードウェア アクセラレーションによってサポートされていない機能は、次のとおりです。

- Threat Defense コンテナインスタンス が有効になっている管理対象デバイス。
- インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまで TLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}** コマンド。

現在のステータスを表示するには、**system support ssl-hw-status** コマンドを使用します。

SSL ハードウェア アクセラレーションでサポートされる暗号のリストを表示するには、**system support ssl-hw-supported-ciphers** コマンドを使用します。

例

SSL ハードウェア アクセラレーションの現在のステータスを表示する例を次に示します。

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

デバイスをリブートするプロンプトを表示して、SSL ハードウェア アクセラレーションを有効にする例を次に示します。

```
If you enable SSL hardware acceleration, you cannot:
    1.    Decrypt passive or inline tap traffic.
    2.    Preserve Do Not Decrypt connections when the inspection engine restarts.
Continue? (y/n) [n]: y


Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]:
 y

SSL hardware acceleration will be enabled on system boot.
```

デバイスをリブートする前に、上記のすべてを確認する必要があります。

SSL ハードウェア アクセラレーションでサポートされる暗号の一部を次に示します。

```
> system support ssl-hw-supported-ciphers
CID     Cipher Suite Name                                CH_mod Keep     Support Inline
 Support Passive
-------------------------------------------------------------------------------------------------------
0x0004  TLS_RSA_WITH_RC4_128_MD5                         Yes             Yes
 Yes
0x0005  TLS_RSA_WITH_RC4_128_SHA                         Yes             Yes
 Yes
0x0009  TLS_RSA_WITH_DES_CBC_SHA                         Yes             Yes
 Yes
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA                    Yes             Yes
 Yes
0x000c  TLS_DH_DSS_WITH_DES_CBC_SHA                      No              No
 No
0x000d  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA                 No              No
 No
0x000f  TLS_DH_RSA_WITH_DES_CBC_SHA                      No              No
 No
0x0010  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA                 No              No
 No
0x0012  TLS_DHE_DSS_WITH_DES_CBC_SHA                     No              No
 No
0x0013  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA                No              No
 No
0x0015  TLS_DHE_RSA_WITH_DES_CBC_SHA                     Yes             Yes
 No
0x0016  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                Yes             Yes
 No
0x0018  TLS_DH_Anon_WITH_RC4_128_MD5                     No              Yes
 No
0x001a  TLS_DH_Anon_WITH_DES_CBC_SHA                     No              Yes
```

```
 No
0x001b  TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA               No              Yes
 No
0x001e  TLS_KRB5_WITH_DES_CBC_SHA                       No              No
 No
0x001f  TLS_KRB5_WITH_3DES_EDE_CBC_SHA                  No              No
 No
0x0020  TLS_KRB5_WITH_RC4_128_SHA                       No              No
 No
0x0024  TLS_KRB5_WITH_RC4_128_MD5                       No              No
 No
0x002f  TLS_RSA_WITH_AES_128_CBC_SHA                    Yes             Yes
 Yes
0x0030  TLS_DH_DSS_WITH_AES_128_CBC_SHA                 No              No
 No
0x0031  TLS_DH_RSA_WITH_AES_128_CBC_SHA                 No              No
 No
… more
```

system support view-files

Cisco Technical Assistance Center（TAC）とともに問題を解決する際に、システムログの内容を表示するには、**system support view-files** コマンドを使用します。

system support view-files

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

system support view-files コマンドは、システムログを開きます。Cisco Technical Assistance Center（TAC）への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、Enter を押します。
- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイルリストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたらSpaceキーを押してログエントリの次のページを表示します。次のログエントリのみを表示するにはEnterを押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。**ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、Ctrl+C を使用します。**
- メニュー構造のレベルを 1 つ上がるには、**b** を入力します。

ログを開いたままにして、新しいメッセージが追加されたときに確認できるようにするには、**tail-logs** コマンドを使用します。

例

次に、ngfw.log ファイルを表示する例を示します。ファイル リストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイル リストが続きます。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
```

```
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

関連コマンド

Command	説明
tail-logs	ログを開き、開いたままにします。

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。