sa - show a

sftunnel-status

デバイスと管理側 Management Center 間の接続（トンネル）のステータスを表示するには、**sftunnel-status** コマンドを使用します。

sftunnel-status

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

デバイスと管理側 Management Center 間の接続（トンネル）のステータスを表示するには、**sftunnel-status** コマンドを使用します。ローカルマネージャである Device Manager を使用している場合、このコマンドを実行しても情報は表示されません。

ステータス情報には、次のセクションが含まれます。

- [SFTUNNEL Status]：接続が確立された時刻、および接続で使用される管理インターフェイスに関する情報。
- [RUN STATUS]：IP アドレス、暗号化、および登録ステータス情報。
- [PEER INFO]：Management Center とこのデバイスへの接続に関する情報。このセクションには、ID、正常性イベント、RPC、NTP、IDS、マルウェアルックアップ、CSM_CCM（デバイスの設定に使用）、eStreamer、UE チャネル、および FSTREAM など、さまざまなサービスのためにシステム間で送信される可能性がある複数のタイプのメッセージの統計ブロックも含まれます。
- [RPC status]。

例

次に、**sftunnel-status** コマンドの出力例を示します。

```
> sftunnel-status

SFTUNNEL Start Time: Tue Oct 11 21:44:44 2016
        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 2
        Reserved SSL connections: 0
        Management Interfaces: 1
        br1 (control events) 10.83.57.37,2001:420:2710:2556:1:0:0:37

**********************

**RUN STATUS****10.83.57.41*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface br1
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface br1
        Registration: Completed.
```

```
        IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
        sw_version 6.2.0
        sw_build 2007
        Management Interfaces: 1
        eth0 (control events) 10.83.57.41,2001:420:2710:2556:1:0:0:41
        Peer channel Channel-A is valid  type (CONTROL), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'
        Peer channel Channel-B is valid  type (EVENT), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'

        TOTAL TRANSMITTED MESSAGES <3> for Identity service
        RECEIVED MESSAGES <2> for Identity service
        SEND MESSAGES <1> for Identity service
        HALT REQUEST SEND COUNTER <0> for Identity service
        STORED MESSAGES for Identity service (service 0/peer 0)
        STATE <Process messages> for Identity service
        REQUESTED FOR REMOTE <Process messages> for Identity service
        REQUESTED FROM REMOTE <Process messages> for Identity service

        TOTAL TRANSMITTED MESSAGES <2760> for Health Events service
        RECEIVED MESSAGES <1380> for Health Events service
        SEND MESSAGES <1380> for Health Events service
        HALT REQUEST SEND COUNTER <0> for Health Events service
        STORED MESSAGES for Health service (service 0/peer 0)
        STATE <Process messages> for Health Events service
        REQUESTED FOR REMOTE <Process messages> for Health Events service
        REQUESTED FROM REMOTE <Process messages> for Health Events service

        TOTAL TRANSMITTED MESSAGES <656> for RPC service
        RECEIVED MESSAGES <328> for RPC service
        SEND MESSAGES <328> for RPC service
        HALT REQUEST SEND COUNTER <0> for RPC service
        STORED MESSAGES for RPC service (service 0/peer 0)
        STATE <Process messages> for RPC service
        REQUESTED FOR REMOTE <Process messages> for RPC service
        REQUESTED FROM REMOTE <Process messages> for RPC service

        TOTAL TRANSMITTED MESSAGES <25131> for IP(NTP) service
        RECEIVED MESSAGES <13532> for IP(NTP) service
        SEND MESSAGES <11599> for IP(NTP) service
        HALT REQUEST SEND COUNTER <0> for IP(NTP) service
        STORED MESSAGES for IP(NTP) service (service 0/peer 0)
        STATE <Process messages> for IP(NTP) service
        REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
        REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

        TOTAL TRANSMITTED MESSAGES <2890> for IDS Events service
        RECEIVED MESSAGES <1445> for service IDS Events service
        SEND MESSAGES <1445> for IDS Events service
        HALT REQUEST SEND COUNTER <0> for IDS Events service
        STORED MESSAGES for IDS Events service (service 0/peer 0)
        STATE <Process messages> for IDS Events service
        REQUESTED FOR REMOTE <Process messages> for IDS Events service
        REQUESTED FROM REMOTE <Process messages> for IDS Events service

        TOTAL TRANSMITTED MESSAGES <4> for Malware Lookup Service service
        RECEIVED MESSAGES <1> for Malware Lookup Service) service
        SEND MESSAGES <3> for Malware Lookup Service service
        HALT REQUEST SEND COUNTER <0> for Malware Lookup Service service
        STORED MESSAGES for Malware Lookup Service service (service 0/peer 0)
        STATE <Process messages> for Malware Lookup Service service
        REQUESTED FOR REMOTE <Process messages> for Malware Lookup Service) service
```

```
        REQUESTED FROM REMOTE <Process messages> for Malware Lookup Service service

        TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
        RECEIVED MESSAGES <186> for CSM_CCM service
        SEND MESSAGES <186> for CSM_CCM service
        HALT REQUEST SEND COUNTER <0> for CSM_CCM service
        STORED MESSAGES for CSM_CCM (service 0/peer 0)
        STATE <Process messages> for CSM_CCM service
        REQUESTED FOR REMOTE <Process messages> for CSM_CCM service
        REQUESTED FROM REMOTE <Process messages> for CSM_CCM service

        TOTAL TRANSMITTED MESSAGES <2907> for EStreamer Events service
        RECEIVED MESSAGES <1453> for service EStreamer Events service
        SEND MESSAGES <1454> for EStreamer Events service
        HALT REQUEST SEND COUNTER <0> for EStreamer Events service
        STORED MESSAGES for EStreamer Events service (service 0/peer 0)
        STATE <Process messages> for EStreamer Events service
        REQUESTED FOR REMOTE <Process messages> for EStreamer Events service
        REQUESTED FROM REMOTE <Process messages> for EStreamer Events service

        Priority UE Channel 1 service

        TOTAL TRANSMITTED MESSAGES <2930> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2919> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        Priority UE Channel 0 service

        TOTAL TRANSMITTED MESSAGES <2942> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2931> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        TOTAL TRANSMITTED MESSAGES <29286> for FSTREAM service
        RECEIVED MESSAGES <14648> for FSTREAM service
        SEND MESSAGES <14638> for FSTREAM service

        Heartbeat Send Time:     Wed Oct 12 21:58:31 2016
        Heartbeat Received Time: Wed Oct 12 21:59:48 2016

**********************

**RPC STATUS****10.83.57.41*************
  'ip' => '10.83.57.41',
  'uuid' => 'c03cb3c2-8fe2-11e6-bce8-8c278d49b0dd',
  'ipv6' => '2001:420:2710:2556:1:0:0:41',
  'name' => '10.83.57.41',
  'active' => '1',
  'uuid_gw' => '',
  'last_changed' => 'Tue Oct 11 19:32:20 2016'

Check routes:
```

関連コマンド

Command	説明
configure manager add	リモートマネージャである Management Center を追加します。

sftunnel-status-brief

デバイスと管理側 Management Center の間の接続（トンネル）の簡単なステータスを表示するには、**sftunnel-status-brief** コマンドを使用します。

sftunnel-status-brief

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

管理接続のステータスを表示するには、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

例

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

関連コマンド

Command	説明
sftunnel-status	管理トンネルステータスの詳細表示を表示します。

show aaa-server

AAA サーバーの統計情報を表示するには、**show aaa-server** コマンドを使用します。

show aaa-server ［ **LOCAL** | *groupname* ［**host** *hostname*］ | **protocol** *protocol*］

構文の説明

groupname	（オプション）グループ内のサーバーの統計情報を表示します。
host *hostname*	（オプション）グループ内の特定のサーバーの統計情報を表示します。
LOCAL	（オプション）ローカルユーザーデータベースの統計情報を表示します。
protocol *protocol*	（オプション）指定したプロトコル（**ldap** または **radius**）のサーバーの統計情報を表示します。

コマンド デフォルト

デフォルトで、すべての AAA サーバー統計情報が表示されます。

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。

使用上のガイドライン

次の表に、**show aaa-server** コマンド出力のフィールドの説明を示します。

フィールド	説明
Server Group	サーバーグループ名。
Server Protocol	サーバーグループのサーバープロトコル。
Server Address	AAA サーバーの IP アドレス。
Server port	システムおよび AAA サーバーによって使用される通信ポート。

フィールド	説明
Server status	サーバーのステータス。ステータスの後に「(admin initiated)」と表示されている場合、このサーバーは、**aaa-server active** または **aaa-server fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。値は次のとおりです。 • ACTIVE：システムはこの AAA サーバーと通信します。 • FAILED：システムはこの AAA サーバーと通信できません。この状態になったサーバーは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。 最終トランザクション日時を次のいずれかの形式で示します。 • `Last Transaction success at` *`time timezone date`* • `Last Transaction failure at` *`time timezone date`* • `Last Transaction at Unknown`（デバイスがサーバーとまだ通信していない場合）
Number of pending requests	現在進行中の要求数。
Average round trip time	サーバーとのトランザクションを完了するまでにかかる平均時間。
Number of authentication requests	システムによって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。
Number of authorization requests	認可要求数。この値は、コマンド認可、コンピュータを通過するトラフィックの認可、トンネルグループでイネーブルにされた WebVPN および IPsec 認可機能が原因の認可要求を指します。タイムアウト後の再送信は、この値には含まれません。
Number of accounting requests	アカウンティング要求数。タイムアウト後の再送信は、この値には含まれません。
Number of retransmissions	内部タイムアウト後にメッセージが再送信された回数。この値は、RADIUS サーバー（UDP）にのみ適用されます。
Number of accepts	成功した認証要求数。
Number of rejects	拒否された要求数。この値には、エラー状態、および実際にクレデンシャルが AAA サーバーから拒否された場合の両方が含まれます。
Number of challenges	最初にユーザー名とパスワードの情報を受信した後に、AAA サーバーがユーザーに対して追加の情報を要求した回数。
Number of malformed responses	この値には特に意味はありません。

フィールド	説明
Number of bad authenticators	この値は、RADIUS にのみ適用されます。 RADIUSパケット内の「authenticator」文字列が破損した回数（まれ）、またはシステム上の共有秘密キーが RADIUS サーバー上のものと一致しない回数。この問題を修正するには、正しいサーバー キーを入力します。
タイムアウトの回数	システムが、AAA サーバーが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。
Number of unrecognized responses	認識できない応答またはサポートしていない応答をシステムが AAA サーバーから受信した回数。たとえば、サーバーからの RADIUS パケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバーからのRADIUS応答パケットが破損していることを意味していますが、まれなケースです。

例

次に、グループ内の特定のサーバーの AAA 統計情報を表示する例を示します。

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC Fri Aug 22
Number of pending requests 20
Average round trip time 4ms
Number of authentication requests 20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 1
Number of accepts 16
Number of rejects 4
Number of challenges 5
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0
```

関連コマンド

コマンド	説明
clear aaa-server statistics	AAA サーバー統計情報をクリアします。

show access-control-config

アクセス コントロール ポリシーに関する要約情報を表示するには、**show access-control-config** コマンドを使用します。

show access-control-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

このコマンドを実行すると、各アクセスコントロールルールの特性を含む、アクセス コントロール ポリシーの概要が表示されます。出力には、アクセス コントロール ポリシーの名前と説明、デフォルトのアクション、セキュリティ インテリジェンス ポリシー、およびアクセスコントロールルールのセットと各アクセスコントロールルールに関する情報が表示されます。また、参照されたSSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイルポリシーの名前、侵入変数セットのデータ、ロギング設定、およびポリシーレベルのパフォーマンス、前処理、一般設定などのその他の詳細設定も表示されます。

情報には、送信元と宛先のポートデータ（ICMPエントリのタイプとコードを含む）および各アクセスコントロールルールに一致した接続数（ヒット数）など、ポリシー関連の接続情報が含まれます。

情報には、URLフィルタリングのブロックアクションおよびインタラクティブ ブロック アクションに使用されるHTMLも表示されます。

Device Manager （ローカルマネージャ）を使用している場合、サポートされていない機能はデフォルト設定の表示になるか、または空の表示になります。Management Centerを使用している場合は、マネージャを使用してこれらの設定を調整できます。CLIを使用して、この出力に表示されているルールやオプションを設定することはできません。マネージャを使用する必要があります。

例

次に、ローカルマネージャであるDevice Manager を使用して管理されるデバイスのアクセス制御の設定例を示します。

```
> show access-control-config

===============[ NGFW-Access-Policy ]===============
Description               :
=================[ Default Action ]=================
Default Action            : Block
Logging Configuration
    DC                    : Enabled
    Beginning             : Disabled
    End                   : Disabled
Rule Hits                 : 0
Variable Set              : Default-Set
```

```
===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Disabled
    DC                    : Disabled

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration     : Disabled
    DC                    : Disabled

=======[ Security Intelligence - DNS Policy ]=======
    Name                  : Default DNS Policy

======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

------------[ Rule: Inside_Inside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : inside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

-----------[ Rule: Inside_Outside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : outside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

=======[ Rule Set: root_category (Built-in) ]=======

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  Do not retry URL cache miss lookup  : No
  Inspect Traffic During Apply        : Yes
Network Analysis and Intrusion Policies
  Initial Intrusion Policy            : Balanced Security and Connectivity
  Initial Variable Set                : Default-Set
  Default Network Analysis Policy     : Balanced Security and Connectivity
Files and Malware Settings
  File Type Inspect Limit             : 1460
```

```
  Cloud Lookup Timeout                : 2
  Minimum File Capture Size           : 6144
  Maximum File Capture Size           : 1048576
  Min Dynamic Analysis Size           : 15360
  Max Dynamic Analysis Size           : 2097152
  Malware Detection Limit             : 10485760
Transport/Network Layer Preprocessor Settings
  Detection Settings
    Ignore VLAN Tracking Connections  : No
  Maximum Active Responses            : No Maximum
  Minimum Response Seconds            : No Minimum
  Session Termination Log Threshold   : 1048576
Detection Enhancement Settings
  Adaptive Profile                    : Disabled
Performance Settings
  Event Queue
    Maximum Queued Events             : 5
    Disable Reassembled Content Checks: False
  Performance Statistics
    Sample time (seconds)             : 300
    Minimum number of packets         : 10000
    Summary                           : False
    Log Session/Protocol Distribution : False
  Regular Expression Limits
    Match Recursion Limit             : Default
    Match Limit                       : Default
  Rule Processing Configuration
    Logged Events                     : 5
    Maximum Queued Events             : 8
    Events Ordered By                 : Content Length
Intelligent Application Bypass Settings
    State                                        : Off
Latency-Based Performance Settings
  Packet Handling                     : Disabled

============[ HTTP Block Response HTML ]============
HTTP/1.1 403 Forbidden
Connection: close
Content-Length: 506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;pa
dding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {col
or:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

関連コマンド

Command	説明
show access-list	アクセスコントロールリスト（ACL）の内容を表示します。

show access-list

アクセスリストのルールおよびヒットカウンタを表示するには、**show access-list** コマンドを使用します。

show access-list ［ *id* ［ *ip_address* | **brief** | **numeric** ］ | **element-count** ］

構文の説明

id	（任意）表示をこの 1 つのアクセスリストに制限する既存のアクセスリストの名前。
ip_address	（任意）このアドレスを持つルールに表示を制限する送信元 IPv4 または IPv6 アドレス。
brief	（任意）アクセスリスト ID、ヒットカウント、および最終ルールヒットのタイムスタンプをすべて 16 進形式で表示します。
numeric	（任意）ACL 名を指定すると、ポートが名前ではなく数値で表示されます。たとえば、www ではなく 80 と表示されます。
element-count	（任意）システムで定義されているすべてのアクセスリストのアクセス コントロール エントリの総数を表示します。

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。
6.6	**numeric** および **element-count** キーワードが追加されました。
7.1	オブジェクトグループの検索が有効になっている場合は、**element-count** の出力にオブジェクトグループの内訳も含まれます。

使用上のガイドライン

アクセス コントロール ポリシーの一部の要素は、拡張アクセスコントロールリスト（ACL）エントリとして構成されます。可能な場合、レイヤ 3 基準に基づいてトラフィックをブロックするアクセスコントロールルールが ACL の拒否ルールになります。信頼アクセスコントロールルールと一致する信頼 ACL ルールが表示されることもあります。

ただし、アクセスコントロールルールで検査が要求されている場合、ルールアクションがブロックの場合でも、ACL エントリは実際にトラフィックを許可します。この許可されたトラフィックは、最終的に不要なトラフィックをブロックできる Snort などの検査エンジンに渡されます。

したがって、**show access-list** に示されている低レベル ACL ルールとデバイスのアクセス コントロール ポリシー ルールの間に 1 対 1 の関係はありません。高度な ACL を使用すると、システムは早期にトラフィックのドロップや信頼の決定を下すことができるため、検査を必要としない接続をできる限り迅速に通過させたり、ドロップしたりできます。

（注） アクセス制御のルールとプレフィルタのルールのヒットカウント情報を表示することが目的の場合は、このコマンドの代わりに **show rule hits** コマンドを使用します。

ACLは、ルートマップやサービスポリシーの一致基準など、他の目的にも使用できます。標準および拡張 ACL は、これらの目的で使用されます。

1つのコマンドに複数のアクセス リスト識別子を入力することによって、一度に複数のアクセス リストを表示できます。

brief キーワードを指定して、アクセス リスト ヒット カウント、ID、およびタイムスタンプ情報を 16 進形式で表示できます。16 進形式で表示されるコンフィギュレーション ID は、3 列に表示され、Syslog 106023 および 106100 で使用されるものと同じ ID です。

アクセス リストが最近変更された場合、リストは出力から除外されます。この場合は、メッセージにそのことが示されます。

（注） 出力には、ACL に含まれる要素の数が表示されます。この番号は、必ずしも ACL 内のアクセス コントロール エントリ (ACE) の数と同じではありません。たとえば、アドレス範囲をもつネットワーク オブジェクトを使用する場合、システムは追加の要素を作成することがありますが、これらの追加要素は出力に含まれません。

クラスタリングのガイドライン

クラスタリングを使用する場合、トラフィックが単一のユニットで受信された場合でも、クラスタリングのダイレクタロジックにより、その他のユニットに ACL のヒットカウントが表示される場合があります。これは予期された動作です。クライアントから直接パケットを受信しなかったユニットは、所有者要求に応じてクラスタ制御リンクを介して転送されたパケットを受信することがあるため、ユニットはパケットを受信ユニットに戻す前に ACL をチェックすることがあります。このため、トラフィックがユニットを通過しなかった場合でも ACL ヒット カウントが増分されます。

例

次に、**show access-list** コマンドの出力例を示します。Device Manager （ローカルまたは「オンボックス」マネージャ）を使用している場合、アクセス コントロール ポリシー用に生成された高度なアクセスリストが表示されます。注釈はシステムによって生成され、アクセス コントロールエントリ（ACE）を理解するのに役立ちます。注釈には関連ルールの名前が表示され、その後にルールから生成されたACEが表示されます。次の例では、注釈が強調表示されています。

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY:
```

```
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xc5a178c1
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xdbc1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x3571535c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x118ef4b4
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 28 advanced trust ip ifc inside1_6 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xc6bfe6b7
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x5fe085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x699725ea
```

```
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xe415bb76
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf9bfd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xf08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x952c7254
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xfc38a46f
access-list NGFW_ONBOX_ACL line 42 advanced trust ip ifc inside1_8 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x3f878e23
access-list NGFW_ONBOX_ACL line 43 advanced trust ip ifc inside1_8 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x48e852ce
access-list NGFW_ONBOX_ACL line 44 advanced trust ip ifc inside1_8 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
access-list NGFW_ONBOX_ACL line 45 remark rule-id 268435457: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 46 remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xea5bdd6e
access-list NGFW_ONBOX_ACL line 48 advanced trust ip ifc inside1_3 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xd7461ffc
access-list NGFW_ONBOX_ACL line 49 advanced trust ip ifc inside1_4 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x6e13508e
access-list NGFW_ONBOX_ACL line 50 advanced trust ip ifc inside1_5 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xfe1fcdd6
access-list NGFW_ONBOX_ACL line 51 advanced trust ip ifc inside1_6 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xa4dba9a8
access-list NGFW_ONBOX_ACL line 52 advanced trust ip ifc inside1_7 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 53 advanced trust ip ifc inside1_8 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xc3c3fafb
access-list NGFW_ONBOX_ACL line 54 remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 55 remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL line 56 advanced deny ip any any rule-id 1 (hitcnt=0)
0x84953cae
>
```

次に、16 進形式で指定されたアクセス ポリシー（ヒット カウントがゼロではない ACE）に関する簡単な情報の例を示します。最初の 2 列には、ID が 16 進形式で表示され、3 番めの列にはヒット カウントがリストされ、4 番めの列には、タイムスタンプ値が 16 進形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。タイムスタンプ値は、最終ヒットの時刻を報告します。ヒット カウントがゼロの場合、情報は表示されません。

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

次に、システムで定義されているすべてのアクセスリストのアクセスコントロールエントリの総数である要素カウントの例を示します。アクセスグループとして割り当てられているアクセスリストの場合、アクセスをグローバルに、またはインターフェイス上で制御するために、（実行コンフィギュレーションの **object-group-search access-control** コマンドで表される）オブジェクトグループ検索を有効にすることで要素カウントを減らすことができます。オブジェクトグループ検索をイネーブルにすると、ネットワークオブジェクトがアクセスコントロールエントリで使用されます。それ以外の場合、オブジェクトはそのオブジェクトに含まれる個々の IP アドレスに展開され、送信元/宛先アドレスのペアごとに個別のエントリが書き込まれます。したがって、5 つの IP アドレスを持つ送信元ネットワークオブジェクトと 6 つのアドレスを持つ宛先オブジェクトを使用する単一のルールは、1 つではなく 30 の要素（5 x 6 エントリ）に展開されます。要素カウントが多いほど、アクセスリストが大きくなり、パフォーマンスに影響を与える可能性が高くなります。

```
> show access-list element-count
Total number of access-list elements: 33934
```

7.1 以降では、オブジェクトグループ検索を有効にしている場合、ルールに含まれるオブジェクトグループの数（OBJGRP）、送信元オブジェクト（SRC OBJ）と宛先オブジェクト（DST OBJ）の数、および追加されたグループと削除されたグループの数に関する追加情報が提供されます。

```
> show access-list element-count
Total number of access-list elements: 892

OBJGRP      SRC OG      DST OG      ADD OG      DEL OG
842         842         842         842         0
```

関連コマンド

Command	説明
clear access-list	アクセス リスト カウンタをクリアします。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show alarm settings

ISA 3000 で各タイプのアラームの構成を表示するには、**show alarm settings** コマンドを使用します。

show alarm settings

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 alarm settings** コマンドの出力例を示します。

```
> show alarm settings

Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds              MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
Input-Alarm 2
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

関連コマンド

Command	説明
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。
show environment alarm-contact	入力アラーム コンタクトのステータスを表示します。

Command	説明
show facility-alarm	トリガーされたアラームのステータス情報を表示します。

show allocate-core

CPU コアの割り当て方法に関する情報を表示するには、**show allocate-core** コマンドを使用します。

show allocate-core { **lina-cpu-percentage** | **lina-mem-percentage** | **profile state** }

構文の説明

lina-cpu-percentage	Lina プロセスに割り当てられた CPU コアの割合を示します。残りのコアは Snort プロセスに割り当てられます。
lina-mem-percentage	Linaプロセスに割り当てられたシステムメモリの割合を示します。残りのメモリは Snort プロセスに割り当てられます。
profile	デバイスで現在動作しているコア割り当てプロファイルを表示します。
state	コア割り当てプロセスが有効になっているか無効になっているかを示します。

コマンド履歴

リリース	変更内容
7.3	このコマンドが追加されました。

使用上のガイドライン

管理ソフトウェアから CPU コア割り当てプロファイルを割り当てることができます。このコマンドを使用して、デバイスで実行されているプロファイルを表示および確認します。可能なプロファイルは次のとおりです。

- default：Lina プロセスと Snort プロセスのコア割り当てのデフォルトスキーム。正確な割り当ては、ハードウェアプラットフォームによって異なります。他のオプションを使用して、割合を決定します。
- ips-heavy：IPS の負荷が高いユースケース用に、より多くの CPU を Snort に割り当てます。30% を Lina、70% を Snort に割り当てます。
- vpn-heavy-prefilter-fastpath：VPN トラフィックを高速パスするプレフィルタポリシーも設定するときに、VPN 負荷の高いユースケース用により多くの CPU を Lina に割り当てます。90% を Lina、10% を Snort に割り当てます。
- vpn-heavy-with-inspection：VPN トラフィックを高速パス処理するプレフィルタポリシーを設定せず、その代わりにアクセス コントロール ポリシーでトラフィックを検査する場合、VPN の多いユースケース用により多くの CPU を Lina に割り当てます。60% を Lina、40% を Snort に割り当てます。

例

次に、Lina CPU とメモリの割合、プロファイル、およびコア割り当ての状態を表示する例を示します。

```
> show allocate-core lina-cpu-percentage

Lina CPU percentage is set to : 48
> show allocate-core lina-mem-percentage

Lina memory percentage is set to : 50
> show allocate-core profile

Core allocation profile is set to : default
> show allocate-core state
Core allocation is disabled
```

show app-agent heartbeat

アプリケーション エージェントのステータスを表示するには、**show app-agent heartbeat** コマンドを使用します。

show app-agent heartbeat

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

アプリケーションエージェントのハートビート通信チャネルは、FXOSシャーシのスーパーバイザと 脅威に対する防御 のアプリケーション エージェント間のリンクの正常性をモニタリングする目的で使用されます。これは、Firepower 4100 または 9300 シリーズ デバイスでハードウェアバイパスを設定する場合に使用されます。脅威に対する防御 ソフトウェアを実行する他のデバイスモデルでは使用されません。

show app-agent heartbeat コマンドを使用して、アプリケーション エージェントのハートビート通信チャネルのステータスを表示します。

例

次に、アプリケーション エージェントのハートビートステータスの例を示します。

```
> show app-agent heartbeat
appagent heartbeat timer 1 retry-count 3
```

関連コマンド

Command	説明
app-agent	アプリケーション エージェントをハードウェアバイパス用に設定します。

show arp

ARP テーブルを表示するには、**show arp** コマンドを使用します。

show arp

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

表示出力には、ダイナミック、スタティック、およびプロキシARPエントリが表示されます。ダイナミックARPエントリには、ARPエントリの秒単位のエージングが含まれています。エージングの代わりに、スタティックARPエントリにはダッシュ（-）が、プロキシARPエントリには「alias」という状態が含まれています。

ARPテーブルには、システム通信に使用されるnlp_int_tapなどの内部インターフェイスのエントリを含めることができます。

例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
> show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

関連コマンド

Command	説明
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config all arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、**show arp-inspection** コマンドを使用します。

show arp-inspection

コマンド履歴

リリース	変更内容
6.1	このコマンドが追加されました。
6.2	ルーテッド モードのサポートが追加されました。

例

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

```
> show arp-inspection
interface                arp-inspection         miss
-------------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

関連コマンド

Command	説明
clear arp statistics	ARP 統計情報をクリアします。
show arp statistics	ARP 統計情報を表示します。
show running-config all arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp statistics

ARP 統計情報を表示するには、**show arp statistics** コマンドを使用します。

show arp statistics

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 arp statistics** コマンドの出力例を示します。

```
> show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

次の表で各フィールドについて説明します。

表 *1 : show arp statistics* のフィールド（続き）

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。
Maximum queued blocks	IP アドレスの解決を待機している間に ARP モジュールにキューイングされた最大ブロック数。
Queued blocks	現在 ARP モジュールにキューイングされているブロック数。
Interface collision ARPs received	すべてのインターフェイスで受信された、インターフェイスの IP アドレスと同じ IP アドレスから送信された ARP パケット数。
ARP-defense gratuitous ARPs sent	ARP-Defense メカニズムの一環としてデバイスによって送信された Gratuitous ARP の数。

フィールド	説明
Total ARP retries	最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。
Unresolved hosts	現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。
Maximum unresolved hosts	最後のクリア後、またはデバイスの起動後に、ARP モジュールに存在した未解決ホストの最大数。

関連コマンド

Command	説明
clear arp statistics	ARP 統計情報をクリアします。
show arp	ARP テーブルを表示します。
show running-config all arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show as-path-access-list

現在のすべての自律システム（AS）パスアクセスリストの内容を表示するには、**show as-path-access-list** コマンドを使用します。

show as-path-access-list ［*number*］

構文の説明

number	（オプション）AS パスアクセスリスト番号を指定します。有効な値は、1 ～ 500 です。

コマンド デフォルト

number 引数を指定しない場合、コマンド出力には、すべての AS パスアクセスリストの内容が表示されます。

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。

例

次に、**show as-path-access-list** コマンドの出力例を示します。

```
> show as-path-access-list
 AS path access list 1

 AS path access list 2
```

show asp cluster counter

クラスタリング環境のグローバル情報またはコンテキストに固有の情報をデバッグするには、**show asp cluster counter** コマンドを使用します。

show asp cluster counter

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 asp cluster counter コマンドは、グローバル DP カウンタおよびコンテキストに固有の DP カウンタを表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。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。

例

次に、**show asp cluster counter** コマンドの出力例を示します。

```
> show asp cluster counter
Global dp-counters:
Context specific dp-counters:
MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

関連コマンド

Command	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp dispatch

パフォーマンス問題の診断に役立つ、デバイスのロードバランス ASP ディスパッチャの統計情報を表示するには、**show asp dispatch** コマンドを使用します。このコマンドは、ハイブリッドポーリング/割り込みモードの Threat Defense Virtual デバイスでのみ使用できます。

show asp dispatch

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 asp dispatch** コマンドの出力例を示します。

```
> show asp dispatch
==== Lina DP thread dispatch stats - CORE 0 ====
Dispatch loop count        :         92260212
Dispatch C2C poll count    :                2
CP scheduler busy          :         14936242
CP scheduler idle          :         77323971
RX ring busy               :          1513632
Async lock global q busy   :           809481
Global timer q busy        :          1958684
SNP flow bulk sync busy    :              174
Purg process busy          :             2838
Block attempts             :         44594355
Maximum timeout specified  :         10000000
Minimum timeout specified  :          1572864
Average timeout specified  :          9999994
Waken up with OK status    :          2476791
Waken up with timeout      :         42117564
Sleep interrupted          :            85753
Number of interrupts       :          2492566
Number of RX interrupts    :          1454442
Number of TX interrupts    :          2492566
Enable interrupt ok        :        174566236
Disable interrupt ok       :        174231423
Maximum elapsed time       :         54082257
Minimum elapsed time       :             6165
Average elapsed time       :          9658532
Message pipe stats         :

Last clearing of asp dispatch: Never

==== Lina DP thread home-ring/interface list - CORE 0 ====
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
>
```

show asp drop

高速セキュリティパスでドロップされたパケットまたは接続をデバッグするには、**show asp drop** コマンドを使用します。

show asp drop ［**flow** ［*flow_drop_reason*］ | **frame** ［*frame_drop_reason*］］

構文の説明

flow [*flow_drop_reason*]	（任意）ドロップされたフロー（接続）を表示します。必要に応じて、特定の理由を指定できます。考えられるフローのドロップ理由のリストを表示するには、? を使用します。
frame [*frame_drop_reason*]	（任意）ドロップされたパケットを表示します。必要に応じて、特定の理由を指定できます。考えられるフレームのドロップ理由のリストを表示するには、? を使用します。

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 asp drop コマンドは、高速セキュリティパスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。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。

考えられるドロップの理由については、https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html にある『show asp drop コマンドの使用方法』を参照してください。

例

次に、**show asp drop** コマンドの出力例を示します。タイムスタンプは、カウンタが最後にクリアされた時間を示しています。

```
> show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                          3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                      4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                         760
  Expired flow (flow-expired)                                           1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                             24
  NAT failed (nat-failed)                                           28739
  NAT reverse path failed (nat-rpf-failed)                          22266
  Inspection failure (inspect-fail)                                 19433
```

```
Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

show asp event

データパスまたは制御パスのイベントキューをデバッグするには、**show asp event** コマンドを使用します。

show asp event {dp-cp | cp-dp}

構文の説明

dp-cp	ASPデータパスからコントロールプレーンに送信されたイベントを表示します。
cp-dp	コントロールプレーンから ASP データパスに送信されたイベントを表示します。

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 asp event コマンドは、データパスおよび制御パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

次に、**show asp event dp-cp** コマンドの出力例を示します。

```
> show asp event dp-cp
DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0           0
Routing Event Queue                          0           0
Identity-Traffic Event Queue                 0           1
PTP-Traffic Event Queue                      0           0
General Event Queue                          0           0
Syslog Event Queue                           0           0
Non-Blocking Event Queue                     0           8
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
Crypto Event Queue                           0         146
HA Event Queue                               0           0
Threat-Detection Event Queue                 0           0
SCP Event Queue                              0           0
ARP Event Queue                              0           1
IDFW Event Queue                             0           0
CXSC Event Queue                             0           0
BFD Event Queue                              0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
crypto-msg            810          0      810        0      810          0
arp-in              17288          0    17288        0    17288          0
identity-traffic        2          0        2        0        2          0
scheduler             239          0      239        0      239          0
```

show asp inspect-dp ack-passthrough

Snort インスペクションをバイパスする空の ACK パケットに関連する統計を表示するには、**show asp inspect-dp ack-passthrough** コマンドを使用します。

show asp inspect-dp ack-passthrough

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

これらの統計をリセットするには、**clear asp inspect-dp ack-passthrough** コマンドを使用します。

例

次に出力例を示します。情報には、ACK パススルーが有効かどうかと次の統計が含まれます。

- バイパスされた ACK パケット：検査のために Snort へ転送されなかった空の ACK パケットの数。
- 送信されたメタ ACK：Snort に送信された後続のデータパケットにピギーバックされた空の ACK の数。同じ方向の後続のデータパケットがより高いシーケンス番号の ACK を持っている場合、以前に保存された空の ACK 情報は必要なく、含まれていないため、この数はバイパスされたパケットの数よりも少ないことがあります。

```
> show asp inspect-dp ack-passthrough

Current running state: Enabled

Packet Statistics:
 ACK packets bypassed                    506
 Meta ACK sent                           506
>
```

show asp inspect-dp egress-optimization

出力最適化（パフォーマンスを向上させる機能）に関する統計情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。

show asp inspect-dp egress optimization

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。

使用上のガイドライン

show asp inspect-dp egress-optimization コマンドは、出力最適化（パフォーマンスを向上させる機能）の対象となる接続についての情報を表示します。出力には、次の情報が表示されます。

- [Current running state]：出力最適化が有効か無効か。
- フロー（フローは 1 つ以上のパケットで構成されます）：
  - [Current]：現在出力最適化の対象となっているフローの数。
  - [Maximum]：検査エンジンが最後に再起動された後、または出力最適化統計情報がクリアされてからの、出力最適化の対象となるフローの合計数。
- パケット：
  - [Processed]：処理されたパケットの合計数。
  - [Excepted]：最初は出力最適化の対象と判断されたが、その後に出力最適化の対象外と判断されたパケットの数。

例

次に、**show asp inspect-dp egress-optimization** コマンドの出力例を示します。

```
> show asp inspect-dp egress-optimization
Current running state: Enabled
Flow:
  current: 1, maximum: 3
  snort-unreachable: 0, snort-unsupported-header: 1, snort-unsupported-verdict: 2
Packet:
  processed: 5
  excepted: 0
```

関連コマンド

コマンド	説明
clear asp inspect-dp egress-optimization	出力最適化の統計情報をクリアします。
show conn state egress_optimization	出力最適化の対象となるフローに関する情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。

show asp inspect-dp snapshot

PDTS（Snort へのデータプレーン送信/受信キュー）リングのスナップショットを表示するには、**show asp inspect-dp snapshot** コマンドを使用します。

show asp inspect-dp snapshot {**config** | **instance** *instance_id* **queue** *queue_id*}

構文の説明

config	PDTS スナップショットのグローバル コンフィギュレーションを表示します。
instance *instance_id*	指定した PDTS コンシューマインスタンス ID のスナップショットを表示します。値は 0 ～ 2147483647 です。
queue *queue_id*	PDTS リングの指定されたデータパス送信キュー ID のスナップショットを表示します。値は 0 ～ 2147483647 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

show asp inspect-dp snapshot コマンドは、PDTS リングスナップショット機能のグローバル コンフィギュレーションを表示します。出力には、次の情報が表示されます。

- Max snapshots：許可される自動スナップショットの最大数。
- Current in use：これまでに保存されたスナップショットの数。
- Interval：同じ PDTS リングで 2 つのスナップショットが許可される期間を指定する時間間隔。
- Auto Snapshot：自動 PDTS スナップショット機能が有効か無効かを表示します。

例

次に、**show asp inspect-dp snapshot config** コマンドの出力例を示します。

```
> show asp inspect-dp snapshot config
Max snapshots  Current in use  Interval (min)  Auto Snapshot
-------------  --------------  --------------  -------------
2              0               5               OFF
```

次に、**show asp inspect-dp snapshot instance** コマンドの出力例を示します。

```
> show asp inspect-dp snapshot instance 2 queue 1
0 packet captured
0 packet shown
```

show asp inspect-dp snort

すべての Snort インスタンスのステータスを表示するには、**show asp inspect-dp snort** コマンドを使用します。

show asp inspect-dp snort [instance *instance_id***]**

構文の説明

instance *instance_id*	特定の Snort インスタンスのステータスを表示します。値は 0 ～ 2147483647 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

このコマンドは、すべての Snort インスタンスのステータスを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。
- Pid：Snort インスタンスプロセス ID。
- Cpu-Usage：Snort インスタンス ID の CPU 使用状況。合計およびユーザー/システム別に出力されます。**注**：このフィールドは、Firepower 2100 シリーズでは表示されません。
- Conns：現在 Snort インスタンスが保持している接続の数。
- Segs/Pkts：Snort インスタンスによって現在処理されているセグメントまたはパケットの数。
- Status：Snort インスタンスのステータス。

例

次に、**show asp inspect-dp snort** コマンドの出力例を示します。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid       Cpu-Usage    Conns      Segs/Pkts  Status
           tot (usr | sys)
-- ----- ---------------- ---------- ---------- ----------
0  9188    0% (  0%|  0%)   0          0        READY
1  9187    0% (  0%|  0%)   0          0        READY
2  9186    0% (  0%|  0%)   0          0        READY
```

次に、Firepower 2010 での **show asp inspect-dp snort** コマンドの出力例を示します。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid   Conns      Segs/Pkts  Status
-- ----- ---------- ---------- ----------
0  30080  40           0        READY
1  30081  14           0        READY
2  30079  20           0        READY
```

show asp inspect-dp snort counters

Snortインスタンスの PDTS 関連 raw カウンタを表示するには、**show asp inspect-dp snort counters** コマンドを使用します。

show asp inspect-dp snort counters [instance *instance_id***] [queues] [rate] [debug] [zeros]**

構文の説明

instance *instance_id*	特定の Snort インスタンスのカウンタを表示します。値は 0 ～ 2147483647 です。
queues	キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。
rate	カウンタのスナップショットを 5 秒間取得して 1 秒に平均化し、カウンタの変化率を示します。
debug	他の方法では表示されない特定のデバッグカウンタが表示されます。
zeros	ゼロカウンタを含むすべてのカウンタが表示されます。

コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

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

このコマンドは、Snort インスタンスの PDTS 関連 raw カウンタを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- Type：カウンタのタイプ。データカウンタ、エラーカウンタ、デバッグカウンタなど。
- Name：カウンタの名前。
- Value：カウンタの判読可能な値。
- Raw-Value：カウンタの raw 値。

カウンタ名：

- Tx Bytes：Lina が Snort インスタンスに送信したバイト数。
- Tx Segs：Lina が Snort インスタンスに送信したフレーム/セグメントの数。

- Rx Bytes：Lina が Snort インスタンスから受信したバイト数。
- Rx Segs：Lina が Snort インスタンスから受信したフレーム/セグメントの数。
- NewConns：Snort インスタンスに送信された接続の数。
- RxQ-Wakeup
- TxQ-Wakeup
- TxQ-LB-Dynamic：PDTS ダイナミック ロード バランシングが開始された回数。
- TxQ-Data-Hi-Thresh：Lina の送信キューの上限しきい値に達した回数。
- RxQ-Full：Lina の受信キューがいっぱいになった回数。
- TxQ-Full：Lina の送信キューがいっぱいになった回数。
- TxQ-Data-Limit：Lina の送信キューのデータ制限に達した回数。
- TxQ-LB-Failed：PDTS ダイナミック ロード バランシングに失敗した回数。
- TxQ-Unavail：Lina の送信キューが使用できなかった回数。
- TxQ-Not-Ready：Lina の送信キューの準備ができていなかった回数。
- TxQ-Suspended：Lina の送信キューが中断された回数。
- RxQ-Unavail：Lina の受信キューが使用できなかった回数。
- RxQ-Not-Ready：Lina の受信キューの準備ができていなかった回数。
- RxQ-Suspended：Lina の受信キューが中断された回数。

例

次に、**show asp inspect-dp snort counters** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 5 debug zeros
SNORT Inspect Instance Counters
Id   QId    Type    Name                              Value      Raw-Value
--   ----   ----    ----                              ---------  ----------
5    All    data    Tx Bytes                           3.3 GB   (3549197468)
5    All    data    Tx Segs                            4.7 M    (4671722)
5    All    data    Rx Bytes                           3.3 GB   (3495936190)
5    All    data    Rx Segs                            4.7 M    (4677344)
5    All    data    NewConns                           11.1 K   (11103)
5    All    debug   RxQ-Wakeup                         0        (0)
5    All    debug   TxQ-Wakeup                         4.7 M    (4655982)
5    All    warn    TxQ-LB-Dynamic                     0        (0)
5    All    warn    TxQ-Data-Hi-Thresh                 0        (0)
5    All    drop    RxQ-Full                           0        (0)
5    All    drop    TxQ-Full                           0        (0)
5    All    drop    TxQ-Data-Limit                     0        (0)
5    All    drop    TxQ-LB-Failed                      0        (0)
5    All    err     TxQ-Unavail                        0        (0)
5    All    err     TxQ-Not-Ready                      0        (0)
5    All    err     TxQ-Suspended                      0        (0)
```

```
5    All    err     RxQ-Unavail                    0         (0)
5    All    err     RxQ-Not-Ready                  0         (0)
5    All    err     RxQ-Suspended                  0         (0)
```

show asp inspect-dp snort counters summary

Snort インスタンスの PDTS 関連カウンタを表示するには、**show asp inspect-dp snort counters summary** コマンドを使用します。カウンタは各インスタンスに集約されます。

show asp inspect-dp snort counters summary [instance *instance_id***] [queues] [rate]**

構文の説明

instance *instance_id*	特定の Snort インスタンスのカウンタを表示します。値は 0 ～ 2147483647 です。
queues	キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。
rate	カウンタの 1 秒間の平均増加数を表示します。現在、1 秒間の平均は、コマンドの最後の呼び出しと現在の呼び出しの間の差分増加に基づいています。これは、差分増加が 1 秒間に 1 回サンプリングされた 5 秒間の移動平均に基づくように変更されます。

コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

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

このコマンドは、Snort インスタンスの PDTS 関連カウンタを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- TxBytes：Lina が Snort インスタンスに送信した合計バイト数。
- TxFrames：Lina が Snort インスタンスに送信したフレーム/セグメントの合計数。
- RxBytes：Lina が Snort インスタンスから受信した合計バイト数。
- RxFrames：Lina が Snort インスタンスから受信したフレーム/セグメントの合計数。
- Conns：Snort インスタンスによって処理された接続の合計数。

例

次に、**show asp inspect-dp snort counters summary** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Counter Summary
Id   QId  TxBytes    TxFrames   RxBytes    RxFrames   Conns
--   ---- ---------- ---------- ---------- ---------- -----
2    All    0          0          0          0          0
```

show asp inspect-dp snort queues

すべてのキューを同じインスタンスに集約するすべての Snort インスタンス（プロセス）のキュー情報を表示するには、**show asp inspect-dp snort queues** コマンドを使用します。

show asp inspect-dp snort queues [instance *instance_id***] [detail] [debug]**

構文の説明

instance *instance_id*	特定の Snort インスタンスのキューを表示します。値は 0 ～ 2147483647 です。
detail	キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。
debug	追加のデバッグ情報も表示されます。

コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

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

このコマンドは、すべてのキューを同じインスタンスに集約するすべての Snort インスタンス（プロセス）のキュー情報を表示します。出力には次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- Rx Queue：Lina の受信キュー。「Used」はデータ量を示し、「util」はキュー使用率を示し、「state」は共有メモリの状態を示します。
- TxQ：Lina の送信キュー。「Used」はデータ量を示し、「util」はキュー使用率を示し、「state」は共有メモリの状態を示します。

Counters:

- RxQ-Size：Lina の受信キューサイズ。
- TxQ-Size：Lina の送信キューサイズ。
- TxQ-Data-Limit：送信キューのデータ制限。このしきい値を超えると、データパケットはドロップされます。パーセンテージは、送信キューのしきい値を示します。

- TxQ-Data-Hi-Thresh：送信キューの高しきい値。このしきい値を超えると、PDTS動的ロードバランシングが開始され、他の Snort インスタンスへのフローのバランシングが試行されます。

例

次に、**show asp inspect-dp snort queues** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Queue Configuration

RxQ-Size:              1   MB
TxQ-Size:            128   KB
TxQ-Data-Limit:      102.4 KB   (80%)
TxQ-Data-Hi-Thresh:   35.8 KB   (28%)

Id QId  RxQ         RxQ    TxQ         TxQ
        (used)      (util) (used)      (util)
-- ---- ---------- ------ ---------- ------
0  All    0         0%       0         0%
1  All    0         0%       0         0%
2  All    0         0%       0         0%
```

show asp inspect-dp snort queue-exhaustion

Snortキューの枯渇が発生した場合の自動スナップショットを表示するには、**show asp inspect-dp snort queue-exhaustion** コマンドを使用します。

show asp inspect-dp snort queue-exhaustion ［**snapshot** *snapshot_id*］［**export** *location*］

構文の説明

snapshot *snapshot_id*	このオプションは、キュー枯渇についての情報を出力する特定のスナップショットを指定します。値は 1 ー 24 の範囲で指定します。
export *location*	スナップショットの内容は、オフボックス分析のために、指定された場所の pcap ファイルにエクスポートされます。

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 asp inspect-dp snort queue-exhaustion コマンドは、Snort キューが枯渇したときに取得されたスナップショットの内容を表示します。選択したスナップショットの内容が表示されます。この出力は、**show capture** コマンドの出力に似ています。

例

次に、**show asp inspect-dp snort queue-exhaustion** コマンドの出力例を示します。

```
> show asp inspect-dp snort queue-exhaustion snapshot 1
102 packets captured
   1: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693143043:693144411(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   2: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693144411:693145779(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   3: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693145779:693147147(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   4: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693147147:693148515(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   5: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693153987:693155355(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172858 64977932>
   6: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
(...output truncated...)
```

show asp load-balance

ロードバランサのキューサイズのヒストグラムを表示するには、**show asp load-balance** コマンドを使用します。

show asp load-balance ［**detail**］

構文の説明

detail	（任意）サンプルで使用されているハッシュバケット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 asp load-balance コマンドは、問題のトラブルシューティングに役立つ場合があります。通常、パケットはインターフェイス受信リングからプルした同じコアによって処理されます。ただし、別のコアが受信したパケットと同じ接続をすでに処理している場合、パケットは、そのコアにキューイングされます。このキューイングによって、他のコアがアイドル状態であっても、ロードバランサ キューが大きくなることがあります。詳細については、**asp load-balance per-packet** コマンドを参照してください。

例

次に、**show asp load-balance** コマンドの出力例を示します。X 軸は異なるキューにキューイングされているパケットの数を表します。Y 軸は、パケットがキューイングされているロード バランサのハッシュ バケットを表します（ヒストグラム バケットを示すヒストグラムのバケットと混同しないでください）。キューを持つハッシュバケットの正確な数を確認するには、**detail** キーワードを使用します。

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes
  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
      |                              #
      |   # #                        # #           #
```

```
|   # #                    # #           #
+---------+---------+---------+---------+---------+---------+----
          10        20        30        40        50        60
                    # of queued jobs per queue
```

関連コマンド

Command	説明
asp load-balance per-packet	マルチコア ASA モデルのコア ロード バランシング方式を変更します。

show asp multiprocessor accelerated- features

高速セキュリティ パス マルチプロセッサ アクセラレーションをデバッグするには、**show asp multiprocessor accelerated-features** コマンドを使用します。

show asp multiprocessor accelerated-features

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 asp multiprocessor accelerated-features コマンドを実行すると、マルチプロセッサの高速化機能のリストが表示されます。このリストは、パフォーマンス上の問題をトラブルシューティングするのに役立ちます。

例

次に、**show asp multiprocessor accelerated-features** コマンドの出力例を示します。

```
> show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations(create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        QOS
        Resource Management
        Routing Lookup
        Shun
        SSL data-path
        Syslogging using UDP transport
        TCP Intercept
        TCP Security Engine
        TCP Transport
        Threat Detection
        Unicast RPF
        WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```

show asp overhead

スピンロックおよび非同期損失の統計情報を追跡および表示するには、**show asp overhead** コマンドを使用します。

show asp overhead ［**sort-by-average**］［**sort-by-file**］

構文の説明

sort-by-average	コールごとの平均サイクル数で結果をソートします。
sort-by-file	ファイル名で結果をソートします。

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 asp overhead** コマンドの出力例を示します。

```
> show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
        since last the MP overhead statistics were last cleared
              File Name Line Function Call             Avg         Cycles      %
----------------------- ---- ----------------------  -----  -------------  -----
```

show asp packet-profile

プレフィルタポリシーによって高速パス処理されたパケット数、大規模なフローとしてオフロードされたパケット数、アクセス制御（Snort）によって完全に評価されたパケット数などを表示するには、**show asp packet-profile** コマンドを使用します。

show asp packet-profile [data-path offload snort]

構文の説明

data-path	データ プレーン パケット プロファイルのカウンタを表示します。
offload	ハードウェア オフロード パケット プロファイルのカウンタを表示します。
snort	Snort パケットプロファイルのカウンタを表示します。

コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

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

脅威に対する防御デバイスを通過する各パケットは、設定されているアクセスポリシー、Snort の判定、およびフローオフロードサポートなどのハードウェア機能に応じて、さまざまな処理段階を経由します。

グローバルカウンタは、これらの統計情報を追跡するために使用され、各セッションの終了時に更新されます。これらのグローバルカウンタは収集され、ヒストグラムの形式で表示されます。任意の時点で、デバイスのブートアップ時または最後の再起動以降にシステムによって処理された累積パケットカウンタがヒストグラムに表示されます。

例

次に、**show asp packet-profile** コマンドの出力例を示します。

```
> show asp packet-profile
Current config state: Enabled

Packets Processed
==================

        hw-dynamic-offload                :                    0
        hw-static-offload                 :                    0
        data-path-trust                   :              1419636
        data-path-snort                   :              3522634
        data-path-snort-bypass-allowedlist :               144496
        data-path-snort-bypass-blockedlist :                    0
        data-path-snort-busy-failopen     :                    0
        data-path-snort-down-failopen     :                   10
```

```
data-path-snort-pre-allowedlist-distribution
-------------------------------------------

        Packets         :    Connections
        [0-3]           :              0
        [4-7]           :           6202
        [8-15]          :          10950
        [16-31]         :           2487
        [32-63]         :             85
        [64-127]        :              0
        [128-255]       :              0
        [256-511]       :              0
        [512-1023]      :              0
        [1024 and above]:              0

data-path-snort-pre-blockedlist-distribution
-------------------------------------------

        Packets         :    Connections
        [0-3]           :              0
        [4-7]           :              0
        [8-15]          :              0
        [16-31]         :              0
        [32-63]         :              0
        [64-127]        :              0
        [128-255]       :              0
        [256-511]       :              0
        [512-1023]      :              0
        [1024 and above]:              0

data-path-snort-post-allowedlist-distribution
-------------------------------------------

        Packets         :    Connections
        [0-3]           :              0
        [4-7]           :              0
        [8-15]          :              0
        [16-31]         :              0
        [32-63]         :              0
        [64-127]        :              0
        [128-255]       :              0
        [256-511]       :              0
        [512-1023]      :              0
        [1024 and above]:              0

offload-post-allowedlist-distribution
-------------------------------------------

        Packets         :    Connections
        [0-3]           :              0
        [4-7]           :              0
        [8-15]          :              0
        [16-31]         :              0
        [32-63]         :              0
        [64-127]        :              0
        [128-255]       :              0
        [256-511]       :              0
        [512-1023]      :              0
        [1024 and above]:              0
>
>
```

show asp rule-engine

tmatch コンパイルプロセスのステータスを確認するには、**show asp rule-engine** コマンドを使用します。

show asp rule-engine

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

次に、アクセスグループとして使用されるアクセスリストのコンパイルが進行中か完了しているのかを確認する例を示します。コンパイル時間は、アクセスリストのサイズによって異なります。時間ステータスの Start（開始）と Completed（完了）は、バッチプロセスであり、モジュールに固有ではないため、すべてのルールに共通です。ほとんどのモジュール要素数がテーブルに表示されます。ステータスには、NAT ルール、ルート、オブジェクト、およびインターフェイスのコンパイルも表示されます。

```
> show asp rule-engine

Rule compilation Status:   Completed
Duration(ms):              421
Start Time:                18:58:34 UTC Apr 7 2021
Last Completed Time:       18:58:44 UTC Apr 7 2021
ACL Commit Mode:           MANUAL
Object Group Search:       DISABLED
Transitional Commit Model: DISABLED

Module    |  Insert   |  Remove   |  Current   |

 NAT      |        90  |        60  |         30  |
 ROUTE    |       107  |        40  |         67  |
 IFC      |        30  |        22  |          8  |
 ACL      |      1446  |       970  |        476  |
```

show asp table arp

高速セキュリティパスの ARP テーブルをデバッグするには、**show asp table arp** コマンドを使用します。

show asp table arp ［**interface** *interface_name*］［**address** *ip_address* ［**netmask** *mask*］］

構文の説明

address *ip_address*	（任意）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（任意）ARPテーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（任意）IP アドレスのサブネット マスクを設定します。

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 arp コマンドがコントロールプレーンの内容を表示するのに対して、**show asp table arp** コマンドは高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
> show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

Command	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

高速セキュリティパスの分類子テーブルをデバッグするには、**show asp table classify** コマンドを使用します。

show asp table classify ［**interface** *interface_name*］［**crypto** | **domain** *domain_name*］［**hits**］［**match** *regexp*］

構文の説明

crypto	（任意）暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。
domain *domain_name*	（任意）特定の分類子ドメインのエントリを表示します。使用可能なドメインのリストについては、CLI のヘルプを参照してください。
hits	（オプション）0 以外のヒット値を持つ分類子エントリを表示します。
interface *interface_name*	（任意）分類子テーブルを表示する特定のインターフェイスを指定します。
match *regexp*	（オプション）正規表現に一致する分類子エントリを表示します。正規表現にスペースが含まれる場合、引用符を使用します。

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 asp table classify コマンドは、高速セキュリティパスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類ルールと対応付けます。それぞれのルールには、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。表示される情報はデバッグの目的でのみ使用されます。また、出力は変更される可能性があります。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。

例

次に、**show asp table classify** コマンドの出力例を示します。

```
> show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
```

```
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

次に、**show asp table classify hits** コマンドの出力例を示します。ヒットカウンタの最後のクリアに関するレコードが示されています。

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
        hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
        mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
        hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
        mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
        hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

次に、レイヤ 2 情報を含む **show asp table classify hits** コマンドの出力例を示します。

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any
...

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
```

```
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

show asp table cluster chash-table

クラスタリングのために高速セキュリティパスの cHash テーブルをデバッグするには、**show asp table cluster chash-table** コマンドを使用します。

show asp table cluster chash-table

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 asp table cluster chash-table コマンドは、高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

次に、**show asp table cluster chash-table** コマンドの出力例を示します。

```
> show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
(...output truncated...)
```

関連コマンド

Command	説明
show asp cluster counter	クラスタ データパス カウンタ情報を表示します。

show asp table interfaces

高速セキュリティパスのインターフェイステーブルをデバッグするには、**show asp table interfaces** コマンドを使用します。

show asp table interfaces

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 asp table interfaces コマンドは、高速セキュリティパスのインターフェイステーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

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

```
> show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20
Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

show asp table network-service

高速セキュリティパスのネットワークサービス オブジェクト テーブルをデバッグするには、**show asp table network-service** コマンドを使用します。

show asp table network-service

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

次に、ネットワークサービス オブジェクト テーブルを表示する例を示します。

```
> show asp table network-service
Per-Context Category NSG:
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
```

```
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
       subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
       subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

show asp table routing

高速セキュリティパスのルーティングテーブルをデバッグするには、**show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show asp table routing ［**vrf** *name* | **all**］ ［**management-only**］［**input** | **output**］［**address** *ip_address* ［**netmask** *mask*］ | **interface** *interface_name*］

構文の説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ（/）に続けてプレフィックス（0～128）を入力し、サブネット マスクを含めることができます。たとえば、「fe80::2e0:b6ff:fe01:3b7a/128」のように入力します。
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（任意）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合は、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。
management-only	管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。
［**vrf** *name*	**all**］	Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してビューを特定の仮想ルータに制限できます。すべての仮想ルータのルーティングテーブルを表示するには、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータのルーティングテーブルを表示します。

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。
6.6	［**vrf** *name*	**all**］ キーワードが追加されました。

使用上のガイドライン

show asp table routing コマンドは、高速セキュリティパスのルーティングテーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。management-only キーワードは、管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
> show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

次の例は、alpha という名前の仮想ルータのルーティングテーブルを示しています。

```
> show asp table routing vrf alpha
Routing table for vrf alpha
route table timestamp: 3916283895
in   1.1.1.1         255.255.255.255 identity
in   1.1.1.0         255.255.255.0   i1
out  255.255.255.255 255.255.255.255 i1
out  1.1.1.1         255.255.255.255 i1
out  1.1.1.0         255.255.255.0   i1
out  224.0.0.0       240.0.0.0       i1
```

関連コマンド

Command	説明
show route	コントロール プレーン内のルーティング テーブルを表示します。

show asp table socket

高速セキュリティパスのソケット情報をデバッグするには、**show asp table socket** コマンドを使用します。

show asp table socket ［*handle*］［**stats**］

構文の説明

handle	ソケットの長さを指定します。
stats	高速セキュリティパスのソケットテーブル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

show asp table socket コマンドは、高速セキュリティ スのソケット情報を表示します。この情報は、高速セキュリティパスのソケットにおける問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

次に、**show asp table socket** コマンドの出力例を示します。

```
Protocol  Socket    Local Address              Foreign Address         State
TCP       00012bac  10.86.194.224:23           0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22           0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443            0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22           171.69.137.139:4190     ESTAB
```

次に、**show asp table socket stats** コマンドの出力例を示します。

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
     checksum errors 0
  Sent:
     total 0
```

```
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
  SSL Close: 117
  SSL Server: 58
  SSL Server Verify: 0
  SSL Client: 0
```

TCP/UDP 統計情報は、送受信したパケットのうち、デバイスで実行またはリッスンしているサービス（Telnet、SSH、HTTPS など）に転送されるパケットの数を示すパケットカウンタです。チェックサムエラーは、計算されたパケットチェックサムがパケットに保存されているチェックサム値と一致しなかった（つまり、パケットが破損した）ため、ドロップされたパケットの数です。NP SSL 統計情報は、受信した各タイプのメッセージの数を示します。ほとんどが、SSL サーバーまたは SSL クライアントインスタンスへの新しい SSL 接続の開始と終了を示します。

関連コマンド

Command	説明
show asp table vpn-context	高速セキュリティ パスの VPN コンテキスト テーブルを表示します。

show asp table vpn-context

高速セキュリティパスの VPN コンテキストテーブルをデバッグするには、**show asp table vpn-context** コマンドを使用します。

show asp table vpn-context ［**detail**］

構文の説明

detail	（任意）VPN コンテキスト テーブルに関する追加の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 asp table vpn-context コマンドは、高速セキュリティ スの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

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

```
> show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネルフロー機能が有効になっている場合の **show asp table vpn-context** コマンドの出力例を示します。

```
> show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。固定の IPsec トンネルフロー機能が有効になっている場合、フラグにはPRESERVEフラグが含まれます。

```
> show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

関連コマンド

Command	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp table zone

高速セキュリティパスのゾーンテーブルをデバッグするには、**show asp table zone** コマンドを使用します。

show asp table zone

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 asp table zone コマンドは、高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。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。

例

次に、**show asp table zone** コマンドの出力例を示します。この例では、is-154 という名前のゾーンは実際にはインラインセットであり、トラフィックゾーンではありません。

```
> show asp table zone
Zone: krjones-passive-security-zone id: 48947
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      passive                       GigabitEthernet0/0

Zone: passive_default_context_0 id: 1
    Security-level: 0
    Context       : single_vf
    Zone member(s):

Zone: is-154 id: 34309
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      out                           GigabitEthernet0/2
      in                            GigabitEthernet0/1
```

関連コマンド

Command	説明
show inline-set	インラインセットを表示します。
show zone	トラフィックゾーンを表示します。

show audit-log

システムの監査ログを表示するには、**show audit-log** コマンドを使用します。

show audit-log

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

このコマンドでは、監査ログが時系列の逆順に表示され、最も新しい監査ログイベントが最初に示されます。

イベントには、システムの更新、権限の問題、設定の変更、ポリシーアプリケーションなどが含まれます。この情報は、Management Center によってリモート管理されるデバイスのみで使用できます。ローカル管理システムの監査ログは空になっています。

例

次の例は、監査ログを示しています。

```
> show audit-log
Audit Log Output:
 time                    :  1476223151 (Tue Oct 11 21:59:11 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Clam update synchronization
from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222646 (Tue Oct 11 21:50:46 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Apply AMP Dynamic Analysis C
onfiguration from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222564 (Tue Oct 11 21:49:24 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Apply Initial_Health_Policy
2016-10-11 18:54:59 from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222563 (Tue Oct 11 21:49:23 2016)
```

```
 event_type             :  notify
 subsystem              :  Health > Health Policy > Apply > Initial_Health_Policy 20
16-10-11 18:54:59 > firepower
 actor                  :  admin
 message                :  Apply
 result                 :  Success
 action_source_ip       :  127.0.0.1
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222508 (Tue Oct 11 21:48:28 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Registration '10.83.57.41'
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222473 (Tue Oct 11 21:47:53 2016)
 event_type             :  Restart
 subsystem              :  NTP Configuration changed
 actor                  :  Default User
 message                :  Restart
 result                 :  Success
 action_source_ip       :  Default User IP
 action_destination_ip  :  Default Target IP
-------------------------------------------------------------
```

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。