show asp ～ show az

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、ユーザー EXEC モードまたは特権 EXEC モードで show as-path-access-list コマンドを使用します。

show as-path-access-list [*name*]

構文の説明

name	（オプション）ASパスアクセスリスト名を指定します。

コマンド デフォルト

name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 モード

次の表に、コマンドを入力できるモードを示します。

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

例

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

```
ciscoasa# show as-path-access-list
AS path access list as-path-acl-1
    deny RTR$
AS path access list as-path-acl-2
    permit 100$
```

<xref> に、各フィールドの説明を示します。

表 *1 : show as-path-access-list* のフィールド

フィールド	説明
ASパスアクセスリスト	AS パス アクセス リスト名を示します。
deny	正規表現が ASCII 文字列としてのルートの AS パスの表現に一致しなくなってから拒否されたパケット数を示します。
permit	正規表現が ASCII 文字列としてのルートの AS パスの表現に一致してから転送されたパケット数を示します。

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、特権 EXEC モードで **show asp cluster counter** コマンドを使用します。

show asp cluster counter

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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。

```
ciscoasa# 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

コマンド	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

パフォーマンスに関する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、特権 EXEC モードで **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/割り込みモードのファイアウォールデバイスでのみ使用できます。

show asp dispatch

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	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。

```
ciscoasa# 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、特権EXECモードで **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。*flow_drop_reason* 引数を使用して、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。 *frame_drop_reason* 引数を使用して、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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.0(8)/7.2(4)/8.0(4)	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれます（ **clear asp drop** コマンドを参照）。また、説明の横にドロップ理由のキーワードが表示されるため、関連キーワードを使用して簡単に **capture asp-drop** コマンドを使用できます。

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。高速セキュリティパスの詳細については、一般的な操作の設定ガイドを参照してください。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。

推奨事項を含む、各ドロップの理由の名称と説明の詳細については、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。

```
ciscoasa# 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
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp drop コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	高速セキュリティパスのドロップ統計情報をクリアします。
show conn	接続に関する情報を表示します。

show asp event dp-cp

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、特権 EXEC モードで **show asp event dp-cp** コマンドを使用します。

show asp event dp-cp [**cxsc msg**]

構文の説明

cxsc msg	（オプション）CXSC イベント キューに送信される CXSC イベント メッセージを示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.1(3)	ルーティング イベント キュー エントリが追加されました。

使用上のガイドライン

show asp event dp-cp 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。データ パスと制御パスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# show asp event dp-cp
DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0        2048
Routing Event Queue                          0           1
Identity-Traffic Event Queue                 0          17
General Event Queue                          0           0
Syslog Event Queue                           0        3192
Non-Blocking Event Queue                     0           4
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
```

```
SRTP Event Queue                            0           0
HA Event Queue                              0           3
Threat-Detection Event Queue                0           3
ARP Event Queue                             0           3
IDFW Event Queue                            0           0
CXSC Event Queue                            0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920       4372
  inspect-sunrp   4005920          0   935295  3070625  4005920       4372
routing              77          0       77        0       77          0
arp-in              618          0      618        0      618          0
identity-traffic   1519          0     1519        0     1519          0
syslog             5501          0     5501        0     5501          0
threat-detection     12          0       12        0       12          0
ips-cplane         1047          0     1047        0     1047          0
ha-msg              520          0      520        0      520          0
cxsc-msg            127          0      127        0      127          0
```

show asp load-balance

ロードバランサキューサイズのヒストグラムを表示するには、特権 EXEC モードで **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	（オプション）ハッシュ バケットの詳細情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

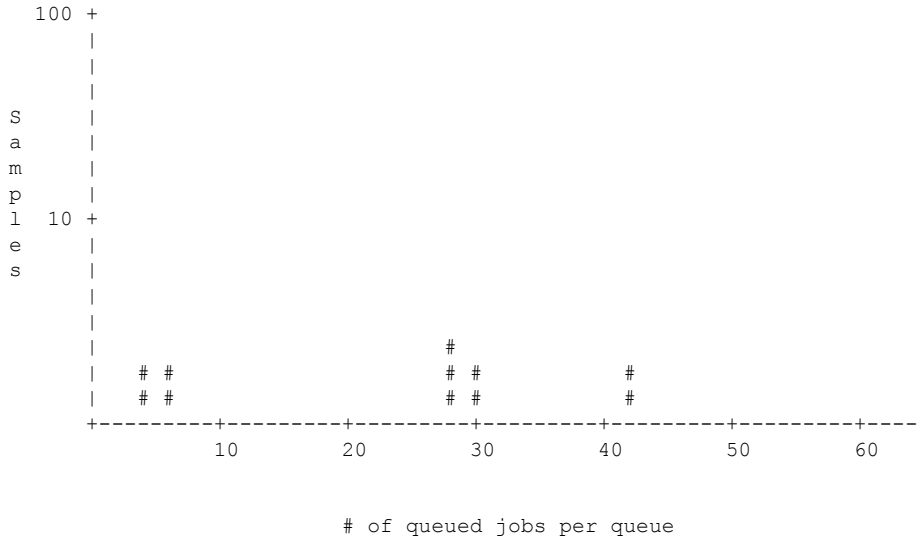
使用上のガイドライン

show 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。

```
ciscoasa# 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
```



次に、 **show asp load-balance detail** コマンドの出力例を示します。

```
ciscoasa# show asp load-balance detail
<Same histogram output as before with the addition of the following values for the
histogram>
Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

関連コマンド

コマンド	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 load-balance per-packet

パケットごとの ASP ロードバランシングの特定の統計情報を表示するには、特権 EXEC モードで **show asp load-balance per-packet** コマンドを使用します。

show asp load-balance per-packet [**history**]

構文の説明

history （オプション）設定ステータス（enabled、disabled、または auto）、現在のステータス（enabled または disabled）、最高水準点と最低水準点、グローバルしきい値、自動切り替えの発生回数、自動スイッチングがイネーブルな場合の最小および最大待機時間、パケットごとの ASP ロードバランシングのタイムスタンプによる履歴、オンおよびオフに切り替える理由を表示します。

コマンド デフォルト

このオプションを指定しない場合は、このコマンドによって、基本ステータス、関連する値、およびパケット単位の ASP ロード バランシングの統計情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

show asp load-balance per-packet コマンドは、パケットごとの ASP ロードバランシングの設定ステータス（enabled、disabled、または auto）、現在のステータス（enabled または disabled）、最高水準点と最低水準点、グローバルしきい値、自動切り替えの発生回数、自動スイッチングがイネーブルな場合の最小および最大待機時間を表示します。

この情報は次の形式で表示されます。

```
Config mode    : [ enabled | disabled | auto ]
Current status : [ enabled | disabled ]
RX ring Blocks low/high watermark      : [RX ring Blocks low watermark in percentage] /
 [RX ring Blocks high watermark in percentage]
System RX ring count low threshold     : [System RX ring count low threshold] / [Total
number of RX rings in the system]
System RX ring count high threshold    : [System RX ring count high threshold] / [Total
 number of RX rings in the system]
```

auto モード

```
Current RX ring count threshold status : [Number of RX rings crossed watermark] / [Total
 number of RX rings in the system]
Number of times auto switched          : [Number of times ASP load-balance per-packet
has been switched]
Min/max wait time with auto enabled    : [Minimal wait time with auto enabled] / [Maximal
 wait time with auto enabled] (ms)
```

手動モード

```
Current RX ring count threshold status : N/A
```

このコマンドの使用は、ASA 5585-X および ASASM でのみサポートされています。

例

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

```
ciscoasa# show asp load-balance per-packet
Config status  : auto
Current status : disabled
RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)
```

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

ciscoasa# **show asp load-balance per-packet history**

Config status : auto

Current status : disabled

RX ring Blocks low/high watermark : 50% / 75%

System RX ring count low threshold : 1 / 33

System RX ring count high threshold : 7 / 33

Current RX ring count threshold status : 0 / 33

Number of times auto switched : 17

Min/max wait time with auto enabled : 200 / 6400 (ms)

==========

From State To State Reason

==========

15:07:13 UTC Dec 17 2013

Manually Disabled Manually Disabled Disabled at startup

15:09:14 UTC Dec 17 2013

Manually Disabled Manually Enabled Config

15:09:15 UTC Dec 17 2013

```
Manually Enabled Auto Disabled 0/33 of the ring(s) crossed the watermark
15:10:16 UTC Dec 17 2013
Auto Disabled Auto Enabled 1/33 of the ring(s) crossed the watermark
Internal-Data0/0 RX[01] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 2/33 of the ring(s) crossed the watermark
Internal-Data0/1 RX[04] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 3/33 of the ring(s) crossed the watermark
Internal-Data0/1 RX[05] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 2/33 of the ring(s) crossed the watermark
Internal-Data0/0 RX[01] dropped below low watermark
15:10:17 UTC Dec 17 2013
Auto Enabled Auto Enabled 3/33 of the ring(s) crossed the watermark
Internal-Data0/2 RX[01] crossed above high watermark
(---More---)
15:14:01 UTC Dec 17 2013
Auto Enabled Auto Disabled 8/33 of the ring(s) crossed the watermark
Internal-Data0/3 RX[01] crossed above high watermark
15:14:01 UTC Dec 17 2013
Auto Disabled Auto Enabled 7/33 of the ring(s) crossed the watermark
Internal-Data0/3 RX[01] dropped below low watermark
(---More---)
15:20:11 UTC Dec 17 2013
Auto Enabled Auto Disabled 0/33 of the ring(s) crossed the watermark
Internal-Data0/2 RX[01] dropped below low watermark
(---More---)
```

関連コマンド

コマンド	説明
asp load-balance per-packet auto	各インターフェイス受信リングまたはフローのセットでのパケットごとの ASP ロード バランシングのオンとオフを自動的に切り替えます。

コマンド	説明
clear asp load-balance history	パケットごとのASPロードバランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。

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、特権EXECモードで **show asp multiprocessor accelerated-features** コマンドを使用します。

show asp multiprocessor accelerated-features

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが導入されました。

使用上のガイドライン

show 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。

```
ciscoasa# 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、特権 EXEC モードで **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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	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。

```
ciscoasa# 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 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、特権 EXEC モードで **show asp rule-engine** コマンドを使用します。

show asp rule-engine [**table classify** { **v4** | **v6** }]

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが導入されました。
9.18(1)	このコマンドが拡張され、IPv4 および IPv6 のルールカウントとコンパイルステータスに関する各表により詳細な情報が追加されました。
9.20(1)	期間情報で、制御された場所でコンパイルが実行された時間とデータパスを分けて表示するようになりました。

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。

```
ciscoasa# show asp rule-engine
Rule compilation Status:   Completed
Duration(ms):              352 (Control: 52, DATAPATH: 300)
Start Time:                17:56:05 UTC Apr 6 2021
Last Completed Time:       17:56:15 UTC Apr 6 2021
ACL Commit Mode:           MANUAL
Object Group Search:       DISABLED
Transitional Commit Model: DISABLED

Module    |  Insert   |  Remove   |  Current   |

 NAT      |       17  |        0  |        17  |
 ROUTE    |       51  |       12  |        39  |
 IFC      |        9  |        0  |         9  |
 ACL      |      426  |        5  |       421  |
```

次に、コンパイルがまだ開始されていない場合の **show asp rule-engine table classify ipv4** コマンドの出力例を示します。

```
firepower(config)# show asp rule-engine table classify v4

-------------------------------------------------------------
Table name        | Rule-count     | Compilation status |
-------------------------------------------------------------
```

```
v4 security       | 8565712        | pending for compile |
-------------------------------------------------------------
v4 input          | 86             | Completed   |
-------------------------------------------------------------
v4 input reverse  | 47             | Completed   |
-------------------------------------------------------------
v4 output         | 36             | Completed   |
-------------------------------------------------------------
v4 output reverse | 3              | Completed   |
-------------------------------------------------------------
```

次に、コンパイルが進行中の場合のコマンドの出力例を示します。

```
firepower(config)# show asp rule-engine table classify v4
-------------------------------------------------------------
Table name        | Rule-count     | Compilation status |
-------------------------------------------------------------
v4 security       | 8565710        | in progress (39%) |
-------------------------------------------------------------
v4 input          | 86             | Completed   |
-------------------------------------------------------------
v4 input reverse  | 45             | Completed   |
-------------------------------------------------------------
v4 output         | 36             | Completed   |
-------------------------------------------------------------
v4 output reverse | 3              | Completed   |
-------------------------------------------------------------
```

次に、コンパイルが完了したときのコマンドの出力例を示します。

```
firepower(config)# show asp rule-engine table classify v4
-------------------------------------------------------------
Table name        | Rule-count     | Compilation status |
-------------------------------------------------------------
v4 security       | 8565712        | Completed   |
-------------------------------------------------------------
v4 input          | 86             | Completed   |
-------------------------------------------------------------
v4 input reverse  | 47             | Completed   |
-------------------------------------------------------------
v4 output         | 36             | Completed   |
-------------------------------------------------------------
v4 output reverse | 3              | Completed   |
-------------------------------------------------------------
```

show asp table cluster chash-table

クラスタハッシュテーブルを表示するには、特権 EXEC モードで **show asp table cluster chash-table** コマンドを使用します。

show asp table cluster chash-table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

同じサイト内のトラフィックをディレクタ ローカリゼーションを使用してローカライズするには、各クラスタのメンバー ユニットで 2 つの追加 cHash テーブルを維持します。1 つのテーブルにはローカル サイト内のすべてのメンバーが含まれ、もう 1 つには現在のユニット以外のすべてのローカル メンバーが含まれます。

例

次に、**show asp table cluster chash-table** コマンドの出力例を示します。サイト 1 にはユニット 0 と 2 があり、サイト 2 にはユニット 1 と 3 があります。次をユニット 0 から表示します。

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
```

```
0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0,
0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0,

Cluster backup chash table:
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,

[...]
```

関連コマンド

コマンド	説明
director-localization	ディレクタ ローカリゼーションをイネーブルにします。

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、特権 EXEC モードで **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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.8(2)	"reference" 情報のコマンド出力が更新されました。

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。高速セキュリティパスの詳細については、CLI コンフィギュレーションガイドを参照してください。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。コマンドの出力の参照値は、特定のエントリのフロー数を表します。

例

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

```
ciscoasa# show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0 reference 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638 reference 1
  10.86.194.172                           Active   0001.03cf.9e79 hits 0 reference 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0 reference 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0 reference 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0 reference 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208 reference
5
```

関連コマンド

コマンド	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、特権 EXEC モードで **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*] [**user-statistics**]

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。
user-statistics	（オプション）ユーザーおよびグループ情報を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)	**hits** オプション、および ASP テーブルのカウンタが最後にクリアされたのがいつかを示すタイムスタンプが追加されました。

リリース	変更内容
8.0(2)	match コンパイルが中止された回数を示すために、新しいカウンタが追加されました。このカウンタは、値が 0 より大きい場合のみ表示されます。
8.2(2)	**match** *regexp* オプションが追加されました。
8.4(4.1)	ASA CX モジュールの **csxc** ドメインおよび **cxsc-auth-proxy** ドメインが追加されました。
9.0(1)	**user-statistics** キーワードが追加されました。出力が更新され、セキュリティ グループ名およびソース タグと宛先タグが追加されました。
9.2(1)	ASA FirePOWER モジュールの sfr ドメインが追加されました。
9.3(1)	出力のセキュリティ グループ タグ（SGT）値が変更されました。タグ値「tag=0」は、「unknow」の予約された SGT 値である 0x0 に完全一致することを示しています。SGT 値「tag=any」は、ルールで考慮する必要がない値を示しています。
9.6(2)	**inspect-m3ua** ドメインが追加されました。

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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# 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
```

次に、セキュリティグループがアクセスリストで指定されていない場合の **show asp table classify** コマンドの出力例を示します。

```
ciscoasa# show asp table classify
```

```
in  id=0x7ffedb54cfe0, priority=500, domain=permit, deny=true
        hits=0, user_data=0x6, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=224.0.0.0, mask=240.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any
```

関連コマンド

コマンド	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 cluster chash-table

高速セキュリティパスの cHash テーブルをクラスタリング用にデバッグするには、特権 EXEC モードで **show asp table cluster chash-table** コマンドを使用します。

show asp table cluster chash-table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:
00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
```

```
33111111
11000112
22332000
00231121
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

関連コマンド

コマンド	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 cts sgt-map

Cisco TrustSec のデータパスに保持されている IP アドレスセキュリティ グループのテーブル データベースから IP アドレスセキュリティ グループのテーブルマップを表示するには、特権 EXEC モードで **show asp table cts sgt-map** コマンドを使用します。

show asp table cts sgt-map ［ **address** *ipv4*［/ *mask* ］ **| address** *ipv6*［/ *prefix* ］ **| ipv4 | ipv6 | sgt** *sgt* ］

構文の説明

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	（任意）特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブルマッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
ipv4	（オプション）IPv4 アドレスのすべての IP アドレス セキュリティ グループのテーブル マップを表示します。
ipv6	（オプション）IPv6 アドレスのすべての IP アドレス セキュリティ グループのテーブル マップを表示します。
sgt *sgt*	（オプション）指定されたセキュリティ グループ テーブルの IP アドレス セキュリティ グループのテーブル マップを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

アドレスが指定されていない場合は、データ パスの IP アドレス セキュリティ グループ テーブル データベース内のすべてのエントリが表示されます。また、セキュリティ グループの名前がある場合は、表示されます。

例

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

```
ciscoasa# show asp table cts sgt-map
IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing
10.34.89.12                         5:Engineering
10.67.0.0\16                        338:HR
192.4.4.4                           345:Finance
Total number of entries shown = 4
```

次に、 **show asp table cts sgt-map address** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map address 10.10.10.5
IP Address                          SGT
============================================
10.10.10.5                          1234:Marketing
Total number of entries shown = 1
```

次に、 **show asp table cts sgt-map ipv6** コマンドの出力例を示します。

```
ciscoasa# show asp table cts sgt-map ipv6
IP Address                                SGT
=========================================================
FE80::A8BB:CCFF:FE00:110                  17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                  18:Eng-Servers
Total number of entries shown = 2
```

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

```
ciscoasa# show asp table cts sgt-map sgt 17
IP Address                                SGT
=========================================
FE80::A8BB:CCFF:FE00:110                  17
Total number of entries shown = 1
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show asp table dynamic-filter

高速セキュリティパスのボットネット トラフィック フィルタ テーブルをデバッグするには、特権 EXEC モードで **show asp table dynamic-filter** コマンドを使用します。

show asp table dynamic-filter [**hits**]

構文の説明

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table dynamic-filter コマンドは、高速セキュリティパス内のボットネット トラフィック フィルタのルールを表示します。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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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 dynamic-filter** コマンドの出力例を示します。

```
ciscoasa# show asp table dynamic-filter
Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
```

```
 Address 10.64.147.16 mask 255.255.255.255 name:
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネットトラフィックフィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネットトラフィックフィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名またはIPアドレスをダイナミックデータベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。

コマンド	説明
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10個のサンプルエントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。 **detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

show asp table filter

高速セキュリティ パス フィルタ テーブルをデバッグするには、特権 EXEC モードで **show asp table filter**コマンドを使用します。

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

構文の説明

acl-name	（オプション）指定されたアクセス リストにインストールされたフィルタを指定します。
hits	（オプション）0 以外のヒット値を持つフィルタ ルールを指定します。
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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

フィルタが VPN トンネルに適用されている場合は、フィルタ テーブルにフィルタ ルールが登録されます。トンネルにフィルタが指定されている場合は、暗号化前および複合化後にフィルタ テーブルがチェックされ、内部パケットを許可または拒否するかが決定されます。

例

次に、user1 が接続する前の **show asp table filter** コマンドの出力例を示します。暗黙拒否ルールのみが着信と発信の両方向で IPv4 および IPv6 にインストールされます。

```
ciscoasa# show asp table filter
Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
         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
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
```

```
        hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
        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
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

次に、user1 が接続した後の **show asp table filter** コマンドの出力例を示します。VPN フィルタ ACL は、着信方向に基づいて定義されます。ソースがピアを表し、宛先は内部リソースを表します。発信ルールは着信ルールのソースと宛先を交換することによって生成されます。

```
ciscoasa# show asp table filter
Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), 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
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
        hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
        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
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=21
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=5001
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
        src ip=95.1.224.100, mask=255.255.255.255, port=5002
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
        src ip=95.1.224.100, mask=255.255.255.255, port=0
```

```
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), 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
out id=0xd616f298, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
        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
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

関連コマンド

コマンド	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 classifier	高速セキュリティパスの分類子の内容を表示します。**S**

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、特権EXECモードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show 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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# 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
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show 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、特権 EXEC モードで **show asp table network-service** コマンドを使用します。

show asp table network-service

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.17(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。

```
ciscoasa# 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 management-only

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、特権EXECモードで **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。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。

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

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、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.3(2)	ゾーンごとのルーティング情報が追加されました。
9.5(1)	管理ルーティング テーブルをサポートするため management-only 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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

（注） 無効なエントリが、ASA 5505 で show asp table routing コマンドの出力に表示される場合があります。

例

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

```
ciscoasa# 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
```

（注） **show asp table routing** コマンドの出力の無効なエントリが ASA 5505 プラットフォームに表示される場合があります。これらのエントリは無視します。これらのエントリは無効です。

関連コマンド

コマンド	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、特権EXECモードでshow asp table socket コマンドを使用します。

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

構文の説明

socket 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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show asp table socket コマンドは、高速セキュリティパ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。高速セキュリティパスの詳細については、CLIコンフィギュレーションガイドを参照してください。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、ハンドルありの **show asp table socket** コマンドの出力例を示します。

```
docs-bxb-asa1/NoCluster/actNoFailover# show asp table socket 123456
Statistics for socket 0x00123456:
2) AM Module
   Mod handle: 0x000000000040545a
   Rx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        App Flow-Ctrl Tx: 0
        Stack:          0x00007fac1cb539c0
        New Conn Cb:    0x0000560fabeeb110
        Notify   Cb:    0x0000560fabeeb500
        App Hdl:        0x00007fac28dcb150
        Shared  Lock:   0x00007fac1685a280
          Group Lock:   0x00007fac1685a280
          Async Lock:   0x00007fac13099640
        Closed Mod Rx: -1, Tx: 3
        Push Module:    INVALID
        State:          LISTEN
        Flags: 0x0
          none
1) SSL Module
   Mod handle: 0x0000000000xxxxxx
   Rx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Upstream Active/peak/total:     0/0/0
        Downstream Active/peak/total:   0/0/0
        Inbound bytes rx/tx:    0/0
        Inbound packets rx/tx:  0/0
        Inbound packets lost:   0
        Outbound bytes rx/tx:   0/0
        Outbound packets rx/tx: 0/0
        Outbound packets lost:  0
        Upstream Close Attempt:         0
        Upstream Close Forced:          0
        Upstream Close Next:            0
        Upstream Close Handshake:       0
        Downstream Close Attempt:       0
        Downstream Close Forced:        0
        Downstream Close Next:          0
        Inbound discard empty buf:      0
        Empty downstream buf:   0
        Encrypt call:           0
        Encrypt call error:     0
        Encrypt handoff:        0
        Encrypt CB success:     0
        Encrypt CB fail:        0
        Flowed Off:             0
        Stats Last State:       0x0 (UNKWN )
        Pending crypto cmds:    0
        Socket Last State:      0x6000 (UNKWN )
        Socket Read State:      0xf0 (read header)
        Handle Read State:      0xf0 (read header)
        References:             NO Session
        In Rekey:               0x0
        Flags:                  0x0
        Header Len:             5
        Record Type:            0x0
        Record Len:             0
        Queued Blocks:          0
        Queued Bytes:           0
0) TM Module
   Mod handle: 0x0000000000xxxxxx
```

```
   Rx:  0/1   ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/1   ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Transp Flow-Ctrl Rx: 0
        TCP handle: 0x0000xxxxxxxxxxx, Interface inside (0x2)
        Connection state is LISTEN
        Local host: 0.0.0.0, Local port: 2444
        Foreign host: 0.0.0.0, Foreign port: 0
        Client host: 0.0.0.0, Client port: 0
        TTL Inbound: 0, TTL Outbound: 255
        Datagrams (MSS: send 536, receive 0):
          Retransmit Queue:     0
          Input Queue:          0
          mis-ordered:          0 (0 bytes)
          Rcvd:                 0
            out of order:       0
            with data:          0
            min ttl drop:       0
            total data bytes:   0
          Sent:                 0
            retransmit:         0
            fastretransmit:     0
            partialack:         0
            Second Congestion:  0
            with data:          0
            total data bytes:   0
```

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、ASA 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

コマンド	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、特権 EXEC モードで **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 デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	トンネルのドロップ後にステートフル フローを保持する各コンテキストの +PRESERVE フラグが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	デバッグ機能を強化するため、次の vpn コンテキスト カウンタが出力に追加されました。 • **Lock Err** ：このカウンタは、VPN コンテキストロックを取得できなかった場合に増加し、このエラーが発生した回数を示します。 • **No SA** ：このカウンタは、VPN コンテキストが処理するパケットを受信したものの、それに対応するアクティブな SA が関連付けられていない場合に増加します。 • **IP Ver Err** ：このカウンタは、不明なバージョンの IP パケットを受信すると増加します。 • **Tun Down** ： VPN コンテキストに関連付けられているトンネルが削除されたか、トンネルハンドルが無効であることを示します。

使用上のガイドライン

show asp table vpn-context コマンドは、高速セキュリティパスの 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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# 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。

```
ciscoasa(config)# 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。

```
ciscoasa# 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
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 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
...
```

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 detail** コマンドの出力例を示します。

```
ciscoasa(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54
Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
VPN CTX  = 0x0005B234
Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
ciscoasa(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
 sysopt VPN CLI.
```

関連コマンド

コマンド	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、特権 EXEC モードで **show asp table zone** コマンドを使用します。

show asp table zone [*zone_name*]

構文の説明

zone_name	（オプション）ゾーン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

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。高速セキュリティパスの詳細については、CLI コンフィギュレーション ガイドを参照してください。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。

```
ciscoasa# show asp table zone
Zone: outside-zone id: 2
 Context: test-ctx
  Zone Member(s) : 2
   outside1       GigabitEthernet0/0
   outside2       GigabitEthernet0/1
```

関連コマンド

コマンド	説明
show asp table routing	デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。

コマンド	説明
show zone	ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

show attribute

VM 属性エージェントとバインディングに関連する情報を表示するには、EXEC モードで **show attribute** コマンドを使用します。

show attribute [**host-map** [**/all**] | **object-map** [**/all**] | **source-group** *agent-name*]

構文の説明

host-map	属性への仮想マシンの IP アドレスの現在のバインディングを表示します。すべての属性のバインディングを確認するには、/all を含めます。たとえば、次のように入力します。 `show attribute host-map /all`
object-map	属性への仮想マシンの IP アドレスの現在のバインディングを表示します。すべての属性のバインディングを確認するには、/all を含めます。たとえば、次のように入力します。 `show attribute host-map /all`
source-group	1 つ以上の属性エージェントの設定および状態を表示します。たとえば、次のように入力します。 `show attribute source-groups agent-name`

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

例

次に、 **show attribute** コマンドの出力例を示します。

```
ciscoasa# show attribute host-map /all
IP Address-Attribute Bindings Information
        Source/Attribute                        Value
=========================================================================
VMAgent.custom.role                           'Developer'
     169.254.107.176
     169.254.59.151
     10.15.28.34
```

```
     10.15.28.32
     10.15.28.31
     10.15.28.33
VMAgent.custom.role                          'Build Machine'
     10.15.27.133
     10.15.27.135
     10.15.27.134
ciscoasa# show attribute object-map /all
Network Object-Attribute Bindings Information
Object
        Source/Attribute                        Value
=========================================================================
dev
    VMAgent.custom.role                         'Developer'
build
    VMAgent.custom.role                         'Build Machine'
ciscoasa# show attribute source-group
Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
       'custom.role ' (2)
```

show auto-update

Auto Update Server のステータスを表示するには、特権 EXEC モードで **show auto-update** コマンドを使用します。

show auto-update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

Auto Update Server のステータスを表示するには、このコマンドを使用します。

例

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

```
ciscoasa(config)# show auto-update
Poll period: 720 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: host name [ciscoasa]
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。

auto-update timeout	タイムアウト期間内にAuto Update Serverに接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

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