CHAPTER 3

show as-path-access-list コマンド～ show auto-update コマンド

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 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。

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。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

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

```
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$
```

表 3-1 に、各フィールドの説明を示します。

表 3-1　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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、一般的な操作のコンフィギュレーション 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 [英語] 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。タイムスタンプが、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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

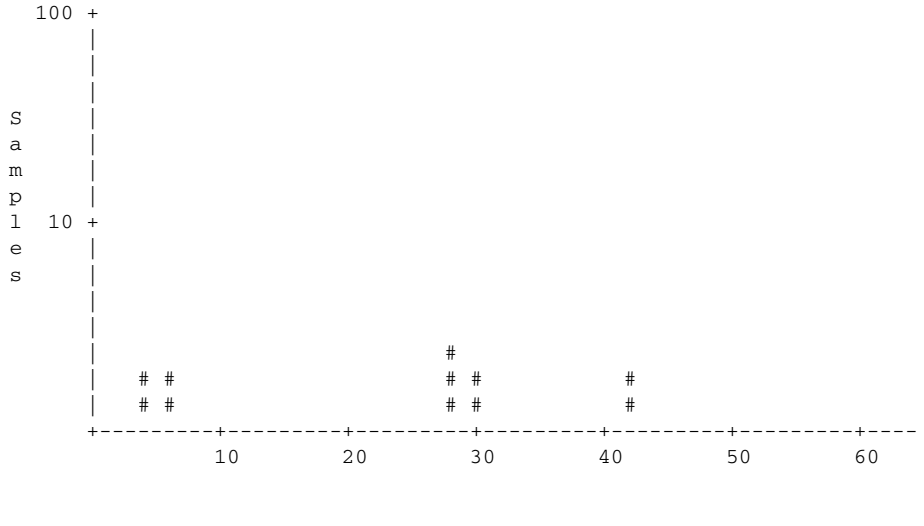
show asp load-balance コマンドは、問題のトラブルシューティングに役立つ場合があります。通常、パケットはインターフェイス受信リングからプルした同じコアによって処理されます。ただし、別のコアが受信したパケットと同じ接続をすでに処理している場合、パケットは、そのコアにキューイングされます。このキューイングによって、他のコアがアイドル状態であっても、ロード バランサ キューが大きくなることがあります。詳細については、**asp load-balance per-packet** コマンドを参照してください。

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。

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。

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

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
```

ASA 5585-X および ASASM だけがこのコマンドの使用をサポートします。

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。
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 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。

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

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** 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/master# 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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)ユーザおよびグループ情報を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。
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。

リリース	変更内容
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 設定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の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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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。
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。

コマンド	説明
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	サーバの IP アドレス、ASA が次にサーバに接続する日時、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 パスのフィルタ 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。
9.3(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 設定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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

```
TCP Statistics:
  Rcvd:
     total14794
     checksum errors0
     no port0
  Sent:
     total0

UDP Statistics:
  Rcvd:
     total0
     checksum errors0
  Sent:
     total0
     copied0

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

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 設定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 フロー機能がイネーブル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
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 フロー機能がイネーブル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
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
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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 設定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。
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。

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

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。

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

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。