show as-path-access-list through show auto-update Commands

show as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the **show as-path-access-list** command in user EXEC or privileged EXEC mode

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

Syntax Description

name	(Optional) Specifies the AS path access list name..

Defaults

If the *name* argument is not specified, command output is displayed for all AS path access lists.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the **show as-path-access-list** command:

```
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$
```

Table 3-1 shows each field description.

Table 3-1 show as-path-access-list Fields

Field	Description
AS path access list	Indicates the AS path access list name.
deny	Indicates the number of packets that are rejected since the regular expression failed to match the representation of the AS path of the route as an ASCII string.
permit	Indicates the number of packets that are forwarded since the regular expression matched the representation of the AS path of the route as an ASCII string.

show asp cluster counter

To debug global or context-specific information in a clustering environment, use the **show asp cluster counter** command in privileged EXEC mode.

show asp cluster counter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show asp cluster counter** command shows the global and context-specific DP counters, which might help you troubleshoot a problem. This information is used for debugging purposes only, and the information output is subject to change. Consult the Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp cluster counter** command:

```
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
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp drop

To debug the accelerated security path dropped packets or connections, use the **show asp drop** command in privileged EXEC mode.

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

Syntax Description

flow [*flow_drop_reason*]	(Optional) Shows the dropped flows (connections). You can specify a particular reason by using the *flow_drop_reason* argument. Use ? to see a list of possible flow drop reasons.
frame [*frame_drop_reason*]	(Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Use ? to see a list of possible frame drop reasons.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.0(8)/7.2(4)/8.0(4)	Output includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command with the associated keyword.

Usage Guidelines

The **show asp drop** command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. See the general operations configuration guide for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

For detailed descriptions of each drop reason name and description, including recommendations, see show asp drop Command Usage.

Examples

The following is sample output from the **show asp drop** command, with the time stamp indicating the last time the counters were cleared:

```
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
```

Related Commands

Command	Description
capture	Captures packets, including the option to capture packets based on an ASP drop code.
clear asp drop	Clears drop statistics for the accelerated security path.
show conn	Shows information about connections.

show asp event dp-cp

To debug the data path or control path event queues, use the **show asp event dp-cp** command in privileged EXEC mode.

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

Syntax Description

cxsc msg	(Optional) Identifies the CXSC event messages that are sent to the CXSC event queue.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.1(3)	A routing event queue entry was added.

Usage Guidelines

The **show asp event dp-cp** command shows the contents of the data path and control path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the data path and control path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp event dp-cp** command:

```
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

To display a histogram of the load balancer queue sizes, use the **show asp load-balance** command in privileged EXEC mode.

show asp load-balance [**detail**]

Syntax Description

detail	(Optional) Shows detailed information about hash buckets.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	This command was added.

Usage Guidelines

The **show asp load-balance** command might help you troubleshoot a problem. Normally a packet will be processed by the same core that pulled it in from the interface receive ring. However, if another core is already processing the same connection as the packet just received, then the packet will be queued to that core. This queuing can cause the load balancer queue to grow while other cores are idle. See the **asp load-balance per-packet** command for more information.

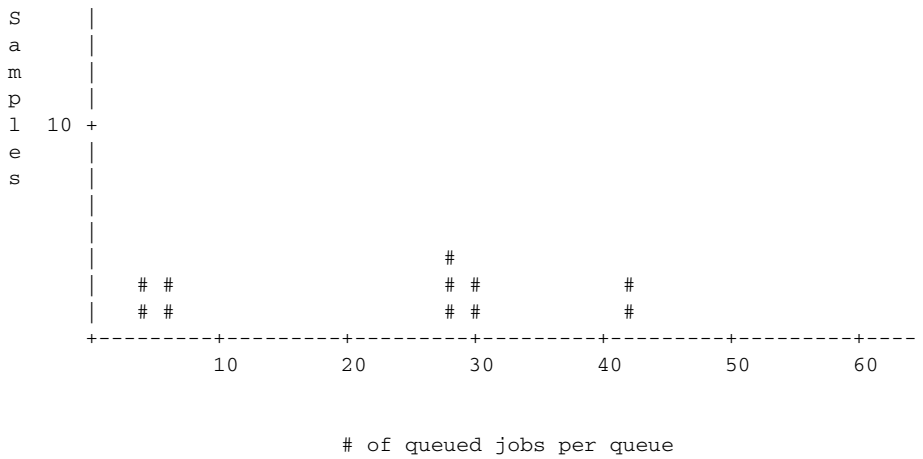
Examples

The following is sample output from the **show asp load-balance** command. The X-axis represents the number of packets queued in different queues. The Y-axis represents the number of load balancer hash buckets (not to be confused with the bucket in the histogram title, which refers to the histogram bucket) that has packets queued. To know the exact number of hash buckets having the queue, use the **detail** keyword.

```
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

  100 +
      |
      |
      |
```



The following is sample output from the **show asp load-balance detail** command.

```
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
```

RelatedCommands

Command	Description
asp load-balance per-packet	Changes the core load balancing method for multi-core ASA models.

show asp load-balance per-packet

To display specific statistics for ASP load balancing per packet, use the **show asp load-balance per-packet** command in privileged EXEC mode.

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

Syntax Description

history	(Optional) Shows the configuration status (enabled, disabled, or auto), current status (enabled or disabled), high and low watermarks, the global threshold, the number of times an automatic switch occurred, the minimum and maximum wait times with automatic switching enabled, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.

Defaults

If you do not specify any options, this command shows the basic status, related values, and statistics of ASP load balancing per packet.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

The **show asp load-balance per-packet** command shows the configuration status (enabled, disabled, or auto), current status (enabled or disabled), high and low watermarks, the global threshold, the number of times an automatic switch occurred, and the minimum and maximum wait times with automatic switching enabled, for ASP load balancing per packet.

The information appears in the following format:

```
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 mode

```
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)
```

Manual mode

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

Only the ASA 5585-X and the ASASM support the use of this command.

Examples

The following is sample output from the **show asp load-balance per-packet** command:

```
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)
```

The following is sample output from the **show asp load-balance per-packet history** command:

```
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---)
```

Related Commands

Command	Description
asp load-balance per-packet auto	Automatically switches ASP load balancing per packet on and off on each interface receive ring or set of flows.
clear asp load-balance history	Clears the history of ASP load balancing per packet and reset the number of times an automatic switch occurred.

show asp table cluster chash-table

To show the cluster hash tables, use the **show asp table cluster chash-table** command in privileged EXEC mode.

show asp table cluster chash-table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

To localize the traffic within the same site using director localization, each cluster member unit maintains two additional cHash tables; one table contains all members in the local site, and the other contains all local members except the current unit.

Examples

The following is sample output from the **show asp table cluster chash** command. Site 1 has unit 0 and 2, and Site 2 has unit 1 and 3. From unit 0, it shows the following:

```
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,

[...]
```

Related Commands

Command	Description
director-localization	Enables director localization.

show asp table arp

To debug the accelerated security path ARP tables, use the **show asp table arp** command in privileged EXEC mode.

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

Syntax Description

address *ip_address*	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask *mask*	(Optional) Sets the subnet mask for the IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.8(2)	The command output was updated for “reference” information.

Usage Guidelines

The **show arp** command shows the contents of the control plane, while the **show asp table arp** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command. The reference value in the command output represents the number of flows for the specific entry,

Examples

The following is sample output from the **show asp table arp** command:

```
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
```

Related Commands

Command	Description
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode.

s**how asp table classify** [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

Syntax Description

crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See the CLI help for a list of the available domains.
hits	(Optional) Shows classifier entries that have non-zero hits values.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.
match *regexp*	(Optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.
user-statistics	(Optional) Specifies user and group information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)	The **hits** option and the timestamp were added to indicate the last time the ASP table counters were cleared.
8.0(2)	A new counter was added to show the number of times a match compilation was aborted. This counter is shown only if the value is greater than 0.
8.2(2)	The **match** *regexp* option was added.
8.4(4.1)	The **csxc** and **cxsc-auth-proxy** domains for the ASA CX module was added.
9.0(1)	The **user-statistics** keyword was added. The output was updated to add security group names and source and destination tags.
9.2(1)	Added the sfr domain for the ASA FirePOWER module.

Release	Modification
9.3(1)	The security group tag (SGT) value has been modified in the output. The tag value “tag=0” indicates an exact match to 0x0, which is the reserved SGT value for “unknown.” The SGT value “tag=any” indicates a value that you do not need to consider in the rule.
9.6(2)	Added the **inspect-m3ua** domain.

Usage Guidelines

The **show asp table classify** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through. The information shown is used for debugging purposes only, and the output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table classify** command:

```
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
...
```

The following is sample output from the **show asp table classify hits** command with a record of the last clearing hits counters:

```
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
```

The following is sample output from the **show asp table classify hits** command that includes Layer 2 information:

```
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
```

The following is sample output from the **show asp table classify** command when a security group is not specified in the access list:

```
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
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table cluster chash-table

To debug the accelerated security path cHash tables for clustering, use the **show asp table cluster chash-table** command in privileged EXEC mode.

show asp table cluster chash-table

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show asp table cluster chash-table** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table cluster chash-table** command:

```
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
```

Related Commands

Command	Description
show asp cluster counter	Shows cluster datapath counter information.

show asp table cts sgt-map

To show the IP address-security group table mapping from the IP address-security group table database that is maintained in the data path for Cisco TrustSec, use the **show asp table cts sgt-map** command in privileged EXEC mode.

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

Syntax Description

address {i*pv4*[*/mask*] */ipv6*[*/prefix*]}	(Optional.) Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
ipv4	(Optional) Shows all of the IP address-security group table mapping for IPv4 addresses.
ipv6	(Optional) Shows all of the IP address-security group table mapping for IPv6 addresses.
sgt *sgt*	(Optional) Shows the IP address-security group table mapping for the specified security group table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.6(1)	The ability to show network mappings was added.

Usage Guidelines

If the address is not specified, then all the entries in the IP address-security group table database in the data path appear. In addition, the security group names appear when available.

Examples

The following is sample output from the **show asp table cts sgt-map** command:

```
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
```

The following is sample output from the **show asp table cts sgt-map address** command:

```
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
```

The following is sample output from the **show asp table cts sgt-map ipv6** command:

```
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
```

The following is sample output from the **show asp table cts sgt-map sgt** command:

```
ciscoasa# show asp table cts sgt-map sgt 17

IP Address                                SGT
============================================
FE80::A8BB:CCFF:FE00:110                  17

Total number of entries shown = 1
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show asp table dynamic-filter

To debug the accelerated security path Botnet Traffic Filter tables, use the **show asp table dynamic-filter** command in privileged EXEC mode.

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

Syntax Description

hits	(Optional) Shows classifier entries which have non-zero hits values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The **show asp table dynamic-filter** command shows the Botnet Traffic Filter rules in the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table dynamic-filter** command:

```
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
...
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show asp table filter

To debug the accelerated security path filter tables, use the **show asp table filter** command in privileged EXEC mode.

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

Syntax Description

acl-name	(Optional) Specifies the installed filter for a specified access list.
hits	(Optional) Specifies the filter rules that have non-zero hits values.
match *regexp*	(optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

When a filter has been applied to a VPN tunnel, the filter rules are installed into the filter table. If the tunnel has a filter specified, then the filter table is checked before encryption and after decryption to determine whether the inner packet should be permitted or denied.

Examples

The following is sample output from the **show asp table filter** command before a user1 connects. Only the implicit deny rules are installed for IPv4 and IPv6 in both the inbound and outbound directions.

```
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
```

The following is sample output from the **show asp table filter** command after a user1 has connected. VPN filter ACLs are defined based on the inbound direction—the source represents the peer and the destination represents inside resources. The outbound rules are derived by swapping the source and destination for the inbound rule.

```
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
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.
show asp table classifier	**S**hows the classifier contents of the accelerated security path.

show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command in privileged EXEC mode.

show asp table interfaces

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table interfaces** command:

```
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
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show asp table routing management-only

To debug the accelerated security path routing tables, use the **show asp table routing** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses. The management-only keyword, displays the number portability routes in the management routing table.

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

Syntax Description

address *ip_address*	Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter the following: `fe80::2e0:b6ff:fe01:3b7a/128`
input	Shows the entries from the input route table.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask *mask*	For IPv4 addresses, specifies the subnet mask.
output	Shows the entries from the output route table.
management-only	Shows the number portability routes in the management routing table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	Routing per zone information was added.
9.5(1)	The management-only keyword to support management routing table was added.

Usage Guidelines

The **show asp table routing** command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command. The management-only keyword, displays the number-portability routes in the management routing table.

Note Invalid entries may appear in the show asp table routing command output on the ASA 5505.

Examples

The following is sample output from the **show asp table routing** command:

```
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
```

Note Invalid entries in the **show asp table routing** command output may appear on the ASA 5505 platform. Ignore these entries; they have no effect.

Related Commands

Command	Description
show route	Shows the routing table in the control plane.

show asp table socket

To help debug the accelerated security path socket information, use the **show asp table socket** command in privileged EXEC mode.

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

Syntax Description

socket handle	Specifies the length of the socket.
stats	Shows the statistics from the accelerated security path socket table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **show asp table socket** command shows the accelerated security path socket information, which might help in troubleshooting accelerated security path socket problems. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table socket** command.

```
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
```

The following is sample output from the **show asp table socket stats** command.

```
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 statistics are packet counters representing the number of packets sent or received that are directed to a service that is running or listening on the ASA, such as Telnet, SSH, or HTTPS. Checksum errors are the number of packets dropped because the calculated packet checksum did not match the checksum value stored in the packet (that is, the packet was corrupted). The NP SSL statistics indicate the number of each type of message received. Most indicate the start and completion of new SSL connections to either the SSL server or SSL client.

Related Commands

Command	Description
show asp table vpn-context	Shows the accelerated security path VPN context tables.

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

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

Syntax Description

detail	(Optional) Shows additional detail for the VPN context tables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(4)	The +PRESERVE flag for each context that maintains stateful flows after the tunnel drops was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	To enhance debug capability, following vpn context counters were added to the output: • **Lock Err**: This counter is incremented when a VPN context lock could not be obtained and indicates the number of times this error is encountered. • **No SA**: This counter increments if VPN context receives a packet to be processed but does not have an active SA associated with it. • **IP Ver Err**: This counter increments when an unknown version of IP packet is received. • **Tun Down**: Indicates that the tunnel associated with the VPN context is deleted or the tunnel handle is invalid.

Usage Guidelines

The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table vpn-context** command:

```
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
...
```

The following is sample output from the **show asp table vpn-context** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag:

```
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
```

The following is sample output from the **show asp table vpn-context detail** command:

```
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
...
```

The following is sample output from the **show asp table vpn-context detail** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag.:

```
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.
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table zone

To debug the accelerated security path zone table, use the **show asp table zone** command in privileged EXEC mode.

show asp table zone [*zone_name*]

Syntax Description

zone_name	(Optional) Identifies the zone name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

The **show asp table zone** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table zone** command:

```
ciscoasa# show asp table zone

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

Related Commands

Command	Description
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show zone	Shows zone ID, context, security level, and members.

show attribute

To display information related to VM attribute agents and bindings, use the **show attribute** command in EXEC mode.

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

Syntax Description

host-map	Displays current bindings of virtual machine IP addresses to attributes. Include /all to see binding for all attributes. For example, enter the following: `show attribute host-map /all`
object-map	Displays current bindings of virtual machine IP addresses to attributes. Include /all to see binding for all attributes. For example, enter the following: `show attribute host-map /all`
source-group	Displays the configuration and state of one or more attribute agents. For example, enter the following: `show attribute source-groups agent-name`

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
EXEC mode	• Yes	• Yes	• Yes	—	—

Examples

The following is sample output from the **show attribute** commands:

```
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

To see the Auto Update Server status, use the **show auto-update** command in privileged EXEC mode.

show auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added..

Usage Guidelines

Use this command to view Auto Update Server status.

Examples

The following is sample output from the **show auto-update** command:

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

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.