

### show asp – show az

- show as-path-access-list, on page 2
- show asp cluster counter, on page 3
- show asp dispatch, on page 4
- show asp drop, on page 6
- show asp event dp-cp, on page 8
- show asp load-balance, on page 10
- show asp load-balance per-packet, on page 12
- show asp multiprocessor accelerated-features, on page 15
- show asp overhead, on page 17
- show asp rule-engine, on page 18
- show asp table cluster chash-table, on page 20
- show asp table arp, on page 22
- show asp table classify, on page 24
- show asp table cluster chash-table, on page 27
- show asp table cts sgt-map, on page 29
- show asp table dynamic-filter, on page 31
- show asp table filter, on page 34
- show asp table interfaces, on page 37
- show asp table network-object, on page 39
- show asp table network-service, on page 42
- show asp table routing management-only, on page 44
- show asp table socket, on page 46
- show asp table vpn-context, on page 49
- show asp table zone, on page 52
- show attribute, on page 53
- show auto-update, on page 55

### 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...

**Command Default** 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:

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

#### 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$
```

<xref> shows each field description.

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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context	text			
	Routed	Transparent	Single	Multiple			
				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 dispatch

To display statistics for the device's load balance ASP dispatcher, which is useful for diagnosing performance issues, use the **show asp dispatch** command in privileged EXEC mode. It is only available for a firewall device in the hybrid poll/interrupt mode.

#### show asp dispatch

**Command Default** No default behavior or values.

#### **Command Modes**

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

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

#### **Command History**

Modification

9.6(2)

Release

This command was introduced.

#### **Examples**

The following is sample output from the show asp dispatch command.

ciscoasa# show asp dispate	n					
==== Lina DP thread dispate	ch	stats	-	CORE	0	
Dispatch loop count	:			92260	)21	12
Dispatch C2C poll count	:					2
CP scheduler busy	:			14936	524	12
CP scheduler idle	:			77323	397	71
RX ring busy	:			1513	363	32
Async lock global q busy	:			808	948	31
Global timer q busy	:			1958	368	34
SNP flow bulk sync busy	:				17	74
Purg process busy	:			2	283	38
Block attempts	:			44594	135	55
Maximum timeout specified	:			10000	000	00
Minimum timeout specified	:			1572	286	54
Average timeout specified	:			9999	999	94
Waken up with OK status	:			2476	579	91
Waken up with timeout	:			42117	756	54
Sleep interrupted	:			85	575	53
Number of interrupts	:			2492	256	56
Number of RX interrupts	:			1454	144	12
Number of TX interrupts	:			2492	256	56
Enable interrupt ok	:		1	L74560	523	36
Disable interrupt ok	:		1	L74231	L42	23

Maximum	elapsed time	:	54082257
Minimum	elapsed time	:	6165
Average	elapsed time	:	9658532
Message	pipe stats	:	

Last clearing of asp dispatch: Never

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

# show asp drop

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

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed	Transparent	Single	Multiple		
				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 <b>clear asp drop</b> command). It also displays the drop reason keywords next to the description, so you can easily use the <b>capture asp-drop</b> command with the associated keyword.					
Usage Guidelines	The <b>show asp drop</b> which might help yo information about th the information outp command.	command shows the packets or connections dropped by the accelerated security path, bu troubleshoot a problem. See the general operations configuration guide for more ne accelerated security path. This information is used for debugging purposes only, and but is subject to change. Consult Cisco TAC to help you debug your system with this				
	For detailed descrip asp drop Command	tions of each drop reason name and description, including recommendations, see show Usage .				
Examples	The following is sar the last time the cou	nple output from the <b>show asp drop</b> command, with the time stamp indicating inters were cleared:				

ciscoasa# <b>show asp drop</b>	
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 (12_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 – show az

### 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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed	Transparent	Single	Multiple		
				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

**s** 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# <b>show asp event dp-cp</b>		
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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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.



# of queued jobs per queue

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
```

Related Commands	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.

**Command Default** 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:

Command Mode	Firewall Mode		Security Context			
	Routed	Transparent	Single	Multiple		
				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 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% : 1 / 33 System RX ring count low threshold System RX ring count high threshold : 7 / 33 Current RX ring count threshold status : 0 / 33 Number of times auto switched : 17 : 200 / 6400 (ms) Min/max wait time with auto enabled 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 multiprocessor accelerated-features

To debug the accelerated security path multiprocessor accelerate, use the **show asp multiprocessor** accelerated-features command in privileged EXEC mode.

show asp multiprocessor accelerated-features

**Command Default** No default behavior or values.

#### **Command Modes**

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

	Command Mode	Firewall Mode	e	Security Context		
		Routed Transparent Single	Single	Multiple		
				Context	System	
	Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes
ommand History	Balaasa	Modificati				1

9.6(2) This command was introduced.

**Usage Guidelines** The **show asp multiprocessor accelerated-features** command shows the lists of features accelerated for multiprocessors, which might help you troubleshoot a performance problem.

#### Examples

The following is sample output from the **show asp multiprocessor accelerated-features** command:

```
ciscoasa# show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations (create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        OOS
```

Resource Management Routing Lookup Shun SSL data-path Syslogging using UDP transport TCP Intercept TCP Security Engine TCP Transport Threat Detection Unicast RPF WCCP Re-direct Above list applies to routed, transparent, single and multi mode.

# show asp overhead

To track and display spin lock and async loss statistics, use the **show asp overhead** command in privileged EXEC mode.

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

Syntax Description	sort-by-average	Sorts the results by average cycles per call
	sort-by-file	Sorts the results by filename

**Command Default** No default behavior or values.

#### **Command Modes**

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

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

Command History	Release	Modification
	9.6(2)	This command was introduced.

#### Examples

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

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

### show asp rule-engine

To see the status of the tmatch compilation process, use the **show asp rule-engine** command in privileged EXEC mode.

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

Command History	Release	Modification
	9.17(1)	This command was introduced.
	9.18(1)	This command was enhanced to include more detailed information about each table regarding their rule-count and compilation status for IPv4 and IPv6.
	9.20(1)	The duration information shows the split between the time compilation was done in the control place compared to the data path.

#### Example

The following example shows whether the compilation of an access list that is used as an access group is in progress or completed. Compilation time depends on the size of the access list. The time status of Start and Completed is common for all rules, because it is a batch process and not specific to modules. Most module element counts will be shown in the table. The status also shows NAT rules, routes, objects, and interface compilation.

```
ciscoasa# show asp rule-engine
Rule compilation Status: Completed
Duration(ms):
                         352 (Control: 52, DATAPATH: 300)
                       17:56:05 UTC Apr 6 2021
Start Time:
Last Completed Time: 17:56:15 UTC Apr 6 2021
ACL Commit Mode: MANUAL
Object Group Search:
                       DISABLED
Transitional Commit Model: DISABLED
Module
         | Insert | Remove
                               | Current
                                            0 |
NAT
                17 |
                                        17 I
                            12 |
                51 |
ROUTE
                                        39
                                            IFC
                 9
                    0 |
                                         9
         426 |
                            5 |
ACL
         421
                                            1
```

Following example shows output of the **show asp rule-engine table classify ipv4** command when compilation is yet to begin:

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

Table name	I	Rule-count	Ι	Compilation	status
v4 securit	y I	8565712		pending for	compile
v4 input		86	Ι	Completed	

v4	input reverse		47		Completed	
v4	output		36		Completed	
v4	output reverse		3		Completed	

Following example shows output of the command when compilation is in progress:

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

Table name	I	Rule-count	I	Compilation status	
v4 security		8565710		in progress (39%)	
v4 input		86		Completed	
v4 input reverse		45		Completed	
v4 output		36		Completed	
v4 output reverse		3		Completed	

Following example shows output of the command when compilation is complete:

			.9-		
Table name	Ι	Rule-count		Compilation	status
v4 security	Ι	8565712		Completed	
v4 input		86		Completed	
v4 input reverse		47		Completed	
v4 output	Ι	36	Ι	Completed	I
v4 output reverse		3		Completed	

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

### 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:

Command Mode	Firewall Mode		Security Context				
	Routed	Transparent	Single	Multiple			
				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-table** command. Site 1 has unit 0 and 2, and Site 2 has unit 1 and 3. From unit 0, it shows the following:

ciscoasa# show asp table cluster chash-table
Cluster current chash table:

2, 2, 0, 0, 2, 2, 2, 2, 2. 2, 2, 2, 2, 2, 2, 2. 2, 2, 2, 2, 2, 0, 0, 0, 2, 2, Ο, 0, 0, Ο, Ο, Ο, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, Ο, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, Ο, Ο, 0, 0, 0, 0, 0, 0, 0, 0, 0, Ο, Ο, Ο, 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, 2. Ο, 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. Ο, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, Ο, 2. 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 2. 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, Ο, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0, Ο, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0, 2, 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.

[...]

### **Related Commands**

ds	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_addr	ess	(Optional) Identifies an IP address for which you want to view ARP table entries. (Optional) Identifies a specific interface for which you want to view the ARP table.						
	interface interg	face_name							
	netmask mask		(Optional) Sets the s	subnet ma	sk for th	e IP address.			
Command Default	No default behavi	or or values.							
Command Modes	The following tab	le shows the	modes in which you	can ente	r the corr	nmand:			
	Command Mode	Firewall M	ode	Secu	rity Conte	ext			
		Routed	Transparent	Singl	e	Multiple	Multiple		
						Context	System		
	Privileged EXEC	• Yes	• Yes	•`	Yes	• Yes	• Yes		
Command History	Release Modifica	ation							
	7.0(1) This command was added.								
	9.8(2) The com	mand output	t was updated for "re	ference" i	nformati	on.			
Usage Guidelines	The <b>show arp</b> command shows the contents of the control plane, while the <b>show asp table arp</b> 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 s	sample outpu	it from the show asp	table ar	<b>p</b> comma	and:			
	ciscoasa# <b>show</b> Context: single 10.86.194.50 10.86.194.1 10.86.194.172	asp table _vf, Inter	<b>arp</b> face: inside	Active Active Active	000f.60 00b0.64 0001.03	6ce.5d46 hits 0 4ea.91a2 hits 6 3cf.9e79 hits 0	reference 0 38 reference 1 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	Active	0000.0000.0000	hits	50208 reference 5

٦

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.

**show 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.				

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed Transparent		Single	Multiple		
				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.

	Release Modification					
	9.0(1) The <b>user-statistics</b> keyword was added. The output was updated to add security group nar source and destination tags.	nes and				
	9.2(1) Added the sfr domain for the ASA FirePOWER module.					
	9.3(1) The security group tag (SGT) value has been modified in the output. The tag value "tag=0" in an exact match to 0x0, which is the reserved SGT value for "unknown." The SGT value "ta indicates a value that you do not need to consider in the rule.	ndicates g=any"				
	9.6(2) Added the <b>inspect-m3ua</b> domain.					
Usage Guidelines	The <b>show asp table classify</b> 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:					
	<pre>biscoasa# show asp table classify interface test: io. 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, 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     dst 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=53, tag=any     dst 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=53, tag=any     dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any     dst ip=0.0.0.0,</pre>					
	<pre>Interface mgmt: Interface mgmt: Interface mgmt: Ints=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0, Nask=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</pre>					

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, 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, 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, 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, 13 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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed	Transparent	Single	Multiple		
				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 2222223 30000102 11222222 23222331 00002223 33111111 11000112 22332000 00231121

I

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 {ipv4 [/n [/prefix ]}	nask] /ipv6	<ul> <li>(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.</li> <li>(Optional) Shows all of the IP address-security group table mapping for IPv4 addresses.</li> <li>(Optional) Shows all of the IP address-security group table mapping for IPv6 addresses.</li> </ul>				
	ipv4						
	ipv6						
	sgt sgt		(Optional) Shows the security group table.	IP address-secur	ity group table ma	pping for the specified	
Command Default	No default behavi	or or values.					
Command Modes	The following tab	le shows the	modes in which you	can enter the cor	nmand:		
	Command Mode	Firewall M	rewall Mode		text		
		Routed	Transparent	Single	Multiple		
					Context	System	
	Privileged EXEC	• Yes	• Yes	• Yes	• Yes	_	
Command History	Release Modifica	ation					
	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 s	ample outpu	it from the show asp	table cts sgt-ma	ap command:		
	ciscoasa# <b>show</b> IP Address 	asp table	<b>cts sgt-map</b> SGT ===================================				

L0.10	.10.5						1234:Marketing
L0.34	.89.12						5:Engineering
L0.67	.0.0\16						338:HR
L92.4	.4.4						345:Finance
rot.al	number	of	entries	shown	=	4	

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

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. No default behavior or values. **Command Default Command Modes** The following table shows the modes in which you can enter the command: Command Mode Firewall Mode Security Context Routed Transparent **Multiple** Single Context System Privileged Yes • Yes • Yes Yes EXEC **Command History Release Modification** 8.2(1)This command was added. The show asp table dynamic-filter command shows the Botnet Traffic Filter rules in the accelerated security **Usage Guidelines** 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 <b>detail</b> keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.

Command	Description
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 (C	<i>acl-name</i> (Optional) Specifies the installed filter for a specified access list.							
	<b>hits</b> (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.								
Command Default	No default behavi	or or values.							
Command Modes	The following tab	le shows the m	nodes in which you	can enter the co	mmand:				
	Command Mode	Firewall Mod	e	Security Con	text				
		Routed	Transparent	Single	Multiple				
					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 <b>show asp table filter</b> command before a user1 connects. Only the implicit deny rules are installed for IPv4 and IPv6 in both the inbound and outbound directions.								
	<pre>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</pre>								

```
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
    id=0xd68366a0, priority=12, domain=vpn-user, deny=false
 in
        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
     id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
 in
        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
    id=0xd6244f30, priority=12, domain=vpn-user, deny=false
 in
        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	Shows 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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed	Transparent	Single	Multiple		
				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 network-object

To debug the accelerated security path network-object tables when using object group search, use the **show** asp table network-object command in privileged EXEC mode.

```
show asp table network-object { source | destination | count } [ match criteria | non-zero-hits
| zero-hits ]
```

Syntax Description	source S	Show entries in	the source network	object table, ind	cluding reference of	count, hit count, and			
	t								
	<b>destination</b> S a	show entries in and the original	the destination network the destination network the destination of the	work object table nation.	e, including referen	nce count, hit count,			
	count S	Show the numb	per of entries in the t	ables.					
	<b>match</b> criteria	When showing The criteria dif	entries in the source fer depending on the	or destination tal	ole, restrict the view	v to the match criteria.			
		• Source—S	Specify the IP addres	ss/mask, such as	A.B.C.D/0-32 or	X:X:X:X::X/0-128			
		• Destination—Specify the hexadecimal ID of the object, then the IP address/mask. You can determine the ID from <b>show access-list</b> or <b>show object-group</b> output. For example: 0xf0000000 192.178.1.4/32							
	<b>non-zero-hits</b> Restrict the list to only those objects that have non-zero hit counts.								
	<b>zero-hits</b> Restrict the list to only those objects that have zero hit counts.								
Command Default	No default behavior or values.								
Command Modes	The following tab	le shows the n	nodes in which you	can enter the con	nmand:				
	Command Mode	Firewall Mod	le	Security Con	text				
		Routed	Transparent	Single	Multiple				
					Context	System			
	Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes			
Command History	Release Modifica	ition							
	9.22 This com	mand was intro	oduced.						
Usage Guidelines	The ASP network access-control.	object table is	s meaningful only if	you enable obje	ct group search: o	bject-group-search			

#### Example

View entries in the source object table. The Key column shows the IP addresses from the source object group. The value column shows the hexadecimal object ID of the object that includes the IP address. Refent is the number of times the address was added to the object table from the same object group. Hitcnt is how often a connection matched the object. Src-og-id-list is a list of other network objects, by hex ID, that contain the same IP address, with the reference count for those objects.

ciscoasa(config) # show asp table network-object source Source Network Object-Group Table: Kev(IP) Value(Objgrp-id) Refcnt Hitcnt src-og-id-list (refcnt) 192.168.1.4/32 0xf0000000 1 1 192.168.1.5/32 0xf0000000 1 0 0xf0000002 (1) 192.168.1.4/32 0xf0050004 1 1

Restrict the view of source objects based on match criteria.

ciscoasa(config)# show asp table network	-object source ma	tch 192.1	68.1.4/32		
Source Network Object-Group Table:					
Key(IP)	Value(Objgrp-id)	Refcnt	Hitcnt	src-og-id-l	ist
(refcnt)					
192.168.1.4/32	0xf0000000	1	1		
192.168.1.4/32	0xf0050004	1	1	0xf000002	(1)

Restrict the view of source objects to objects that have non-zero hit counts.

ciscoasa(config) # show asp table network	-object source no	n-zero-hi	ts	
Source Network Object-Group Table:				
Key(IP)	Value(Objgrp-id)	Refcnt	Hitcnt	src-og-id-list
(refcnt)				
192.168.1.4/32	0xf0000000	1	1	
192.168.1.4/32	0xf0050004	1	1	0xf0000002 (1)

View entries in the destination object table. The Key column shows the network object ID and IP addresses from the source object group. The value column shows the hexadecimal object ID of the destination object for the access control rule. Refent is the number of times the address was added to the object table from the same object group. Hitcnt is how often a connection matched the object. Src-og-id-list the list of corresponding source object groups by the hex ID of the objects from the ACLs.

ciscoasa(config) # show asp table network-object destination Destination Network Object-Group Table: Value(dst-og-id) Refcnt Hitcnt Key(og id + network) src-og-id-list (refcnt) 0xf000001 0xf0000000 + 192.178.1.4/32 2 1 0xf0000000 (2) 0xf0050004 + 192.178.1.5/32 0xf000003 1 0 0xf0000002 (1)

Restrict the view of destination objects based on match criteria.

ciscoasa(config) # show asp table network-object destination match 0xf0000000 192.178.1.4/32

Destination Netw	ork Object-Group Table:					
Key(og_id + netw	ork)	Value(dst-og-id)	Refcnt	Hitcnt	src-og-id-l	ist
(refcnt)						
0xf0000000 + 192	.178.1.4/32	0xf000001	2	1	0xf0000000	(2)

Related Commands	Command	Description
	object-group-search access-control	Enable object group search for access control rules.
	show asp drop	Shows the accelerated security path counters for dropped packets.

### show asp table network-service

To debug the accelerated security path network-service object tables, use the **show asp table network-service** command in privileged EXEC mode.

#### show asp table network-service

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:

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

**Command History** 

Modification

9.17(1) This command was introduced.

#### Example

Release

The following example shows how to display the network-service object table:

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

subnet=0.0.0.0/0, branch id=840741, branch name=fbcdn-photos-b-a.akamaihd.net., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=840741, branch name=fbcdn-photos-b-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1014669, branch name=fbstatic-a.akamaihd.net., ip\_prot=0, port=0/0x0, source, domain, nsg\_id=512, hits=0 subnet=0.0.0.0/0, branch id=1014669, branch name=fbstatic-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1098051, branch name=fbexternal-a.akamaihd.net., ip\_prot=0, port=0/0x0, source, domain, nsg\_id=512, hits=0 subnet=0.0.0.0/0, branch\_id=1098051, branch\_name=fbexternal-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1217875, branch name=fbcdn-profile-a.akamaihd.net., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=1217875, branch name=fbcdn-profile-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1379985, branch name=fbcdn-creative-a.akamaihd.net., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch\_id=1379985, branch\_name=fbcdn-creative-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsq id=1, hits=0 subnet=0.0.0.0/0, branch id=1524617, branch name=channel.facebook.com., ip\_prot=0, port=0/0x0, source, domain, nsg\_id=512, hits=0 subnet=0.0.0.0/0, branch id=1524617, branch name=channel.facebook.com., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1683343, branch\_name=fbcdn-dragon-a.akamaihd.net., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=1683343, branch name=fbcdn-dragon-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=1782703, branch name=contentcache-a.akamaihd.net., ip\_prot=0, port=0/0x0, source, domain, nsg\_id=512, hits=0 subnet=0.0.0.0/0, branch id=1782703, branch name=contentcache-a.akamaihd.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch\_id=1868733, branch\_name=facebook.net., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=1868733, branch name=facebook.net., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch id=2068293, branch name=plus.google.com., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=2068293, branch name=plus.google.com., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0 subnet=0.0.0.0/0, branch\_id=2176667, branch\_name=instagram.com., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0 subnet=0.0.0.0/0, branch id=2176667, branch name=instagram.com., ip prot=0, port=0/0x0, destination, domain, nsg\_id=1, hits=0 subnet=0.0.0.0/0, branch id=2317259, branch name=linkedin.com., ip prot=0, port=0/0x0, source, domain, nsg id=512, hits=0

subnet=0.0.0.0/0, branch\_id=2317259, branch\_name=linkedin.com., ip prot=0, port=0/0x0, destination, domain, nsg id=1, hits=0

# show asp table routing management-only

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:fe0	01:3b7a/128			
	input		Shows the entries fro	om the input rout	e table.		
	interface interg	face_name	(Optional) Identifies a table.	a specific interfac	e for which you war	nt to view the routing	
	netmask mask		For IPv4 addresses, s	specifies the sub-	net mask.		
	output		Shows the entries fro	om the output rou	ite table.		
	management-onl	management-only Shows the number portability routes in the management routing table.					
Command Default	No default behavior or values.						
Command Modes	- The following tab	le shows th	e modes in which you	can enter the co	mmand:		
	Command Mode Firewall N		Node Security C		ontext		
		Routed	Transparent	Single	Multiple		
					Context	System	
	Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes	
Command History	Release Modifica	ation					
	7.0(1) This command was added.						
	9.3(2) Routing	per zone in	formation was added.				
	9.5(1) The mar	agement-or	nly keyword to support	management ro	uting table was adde	ed.	
Usage Guidelines	The <b>show asp ta</b> which might help	b <b>le routing</b> you trouble	command shows the r shoot a problem. See t	outing table con the CLI configur	tents of the accelera ation guide for more	ted security path, e 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:

cisco	basa# <b>show asp ta</b>	able 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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode		Security Context			
	Routed Transparent		Single	Multiple		
				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:*	LISTEN
TCP	0001c124	10.86.194.224:22	0.0.0:*	LISTEN
SSL	00023b84	10.86.194.224:443	0.0.0:*	LISTEN
SSL	0002d01c	192.168.1.1:443	0.0.0:*	LISTEN
DTLS	00032b1c	10.86.194.224:443	0.0.0:*	LISTEN
SSL	0003a3d4	0.0.0:443	0.0.0:*	LISTEN
DTLS	00046074	0.0.0:443	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 with handle command.

docs-bxb-asal/NoCluster/actNoFailover# show asp table socket 123456
Statistics for socket 0x00123456:

2)	AM Module				
,	Mod handle: 0x00000000004054	5a			
	Rx: 0/3 (0 gueued), Flow-	Ctrl:	Ο,	Tot:	0
	Tx: 0/3 (0 queued), Flow-	Ctrl:	0,	Tot:	0
	App Flow-Ctrl Tx: 0				
	Stack: 0x00007f	ac1cb539c0			
	New Conn Cb: 0x000056	0fabeeb110			
	Notify Cb: 0x000056	0fabeeb500			
	App Hdl: 0x00007f	ac28dcb150			
	Shared Lock: 0x00007f	ac1685a280			
	Group Lock: 0x00007f	ac1685a280			
	Async Lock: 0x00007f	ac13099640			
	Closed Mod Rx: -1, Tx:	3			
	Push Module: INVALID				
	State: LISTEN				
	Flags: 0x0				
1.	none				
⊥)	SSL Module				
	Mod nandle: 0x000000000xxxx	XX Chwl	0	mat .	0
	Kx: 0/10 (0 queued), Flow-	Ctrl:	0,	TOL:	0
	Instroom Active (peak /te	·CUII:	0, (0/0	100:	0
	Downstream Active/peak/cc	/total: 0/	0/0		
	Inhound bytes rx/tx.	0/0	070		
	Inbound packets rx/tx:	0/0			
	Inbound packets lost:	0			
	Outbound bytes rx/tx:	0/0			
	Outbound packets rx/tx:	0/0			
	Outbound packets lost:	0			
	Upstream Close Attempt:	0			
	Upstream Close Forced:	0			
	Upstream Close Next:	0			
	Upstream Close Handshak	.e: 0			
	Downstream Close Attemp	ot: 0			
	Downstream Close Forced	l: 0			
	Downstream Close Next:	0			
	Inbound discard empty b	our: U			
	Emply downstream bul:	0			
	Encrypt call error:	0			
	Encrypt handoff:	0			
	Encrypt CB success:	0			
	Encrypt CB fail:	0			
	Flowed Off:	0			
	Stats Last State:	0x0 (UNKWN	1)		
	Pending crypto cmds:	0			
	Socket Last State:	0x6000 (UN	IKWN	)	
	Socket Read State:	0xf0 (read	l hea	ader)	
	Handle Read State:	0xf0 (read	l hea	ader)	
	References:	NO Session	1		
	In Rekey:	0x0			
	Flags:	UXU			
	Record Type:	5 0⊽0			
	Record Lep.	0			
	Queued Blocks:	0			
	Queued Bytes:	0			
0)	TM Module	-			
- /	Mod handle: 0x000000000xxxx	xx			
	Rx: 0/1 ( 0 queued), Flow-	Ctrl:	Ο,	Tot:	0
	Tx: 0/1 ( 0 queued), Flow-	Ctrl:	Ο,	Tot:	0
	Transp Flow-Ctrl Rx: 0				
	TCP handle: 0x0000xxxxx	xxxxxxx, In	ter	face insid	de (0x2)
	Connection state is LIS	TEN			

```
Local host: 0.0.0.0, Local port: 2444
Foreign host: 0.0.0.0, Foreign port: 0
Client host: 0.0.0.0, Client port: 0
TTL Inbound: 0, TTL Outbound: 255
Datagrams (MSS: send 536, receive 0):
 Retransmit Queue:
                      0
 Input Queue:
                      0
                     0 (0 bytes)
 mis-ordered:
 Rcvd:
                     0
   out of order:
                     0
   with data:
                      0
   min ttl drop:
                      0
   total data bytes: 0
  Sent:
                      0
   retransmit:
                     0
                     0
   fastretransmit:
   partialack:
                      0
   Second Congestion: 0
   with data:
                       0
   total data bytes:
                       0
```

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

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
 Rcvd:
     total O
     checksum errors 0
  Sent:
    total O
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
  SSL Close: 117
  SSL Server: 58
  SSL Server Verify: 0
  SSL Client: 0
```

TCP/UDP 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. No default behavior or values. **Command Default Command Modes** The following table shows the modes in which you can enter the command: Command Mode Firewall Mode Security Context Routed Transparent Single **Multiple** Context System Privileged Yes • Yes • Yes Yes • Yes EXEC **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. The show asp table vpn-context command shows the VPN context contents of the accelerated security path, **Usage Guidelines** 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=000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=000000061, gc=2
VPN ID=005815161168, ENCR+ESP, UP, pk=0000305043, rk=000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=000000061, 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=000000000, gc=0 VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=000000000, 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]
        = UP
State
Flags
        = DECR+ESP
        = 0 \times 0.37928 F0
SA
SPI
        = 0 \times EA0F21F0
       = 0
Group
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
        = ENCR+ESP
Flags
        = 0x037B4B70
SA
SPT
        = 0 \times 900 FDC32
        = 0
Group
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 Er	r=	= 0
Tun Down	=	0
Bad SPI	=	0
Spoof	=	0
Bad Crypt	0	= 0
Rekey Pkt	5	= 0
Rekey Cal	.1	= 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 Er	r=	= 0
Tun Down	=	0
Bad SPI	=	0
Spoof	=	0
Bad Crypt	0	= 0
Rekey Pkt	;	= 0
Rekey Cal	.1	= 0
ciscoasa	(cc	onfig)#
Configura	iti	ion and Restrictions
This conf	ic	guration option is subject to the same CLI configuration restrictions as other
sysopt VE	N	CLL

### **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.

**Command Default** No default behavior or values.

#### **Command Modes**

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

Command Mode	Firewall Mode	9	Security Context		
	Routed	Transparent	Single Multiple		
				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:

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

### Examples

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

ciscoasa# <b>show attribute host-map /all</b> 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:					
	Command Mode	Firewall Mode		Security Context		
		Routed	Transparent	Single	Multiple	
					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 <b>show auto-update</b> command:					
	ciscoasa(config) <b># show auto-update</b> 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						

I