sa - show a

sftunnel-status

To view the status of the connection (tunnel) between the device and the managing management center, use the **sftunnel-status** command.

sftunnel-status

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the **sftunnel-status** command to view the status of the connection between the device and the managing management center. If you are using the local manager, device manager, this command does not provide any information.

Status information includes the following sections:

- SFTUNNEL Status—When the connection was establish and information about management interfaces used in the connection.
- RUN STATUS—IP address, encryption, and registration status information.
- PEER INFO—Information about the management center and its connection to this device. This section also includes statistics blocks for several types of messages that might be transmitted between the systems for various services, including Identity, Health Events, RPC, NTP, IDS, Malware Lookup, CSM_CCM (used for configuring the device), EStreamer, UE Channel, and FSTREAM.
- RPC status.

Examples

The following is sample output from the **sftunnel-status** command.

```
> sftunnel-status

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

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

**RUN STATUS****10.83.57.41*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface br1
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface br1
        Registration: Completed.
        IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
        sw_version 6.2.0
```

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

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

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

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

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

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

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

        TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
        RECEIVED MESSAGES <186> for CSM_CCM service
```

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

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

        Priority UE Channel 1 service

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

        Priority UE Channel 0 service

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

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

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

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

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

Check routes:
```

Related Commands

Command	Description
configure manager add	Adds a remote manager, management center.

sftunnel-status-brief

To view a brief status of the connection (tunnel) between the device and the managing management center, use the **sftunnel-status-brief** command.

sftunnel-status-brief

Command History

Release	Modification
6.7	This command was introduced.

Usage Guidelines

Enter the **sftunnel-status-brief** command to view the management connection status. You can also use **sftunnel-status** to view more complete information.

Examples

See the following sample output for a connection that is down; there is no peer channel "connected to" information, nor heartbeat information shown:

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

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

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

Related Commands

Command	Description
sftunnel-status	Shows a detailed display of the management tunnel status.

show aaa-server

To display statistics for AAA servers, use the **show aaa-server** command.

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

Syntax Description

groupname	(Optional) Show statistics for servers in a group.
host *hostname*	(Optional) Show statistics for a particular server in the group.
LOCAL	(Optional) Show statistics for the LOCAL user database.
protocol *protocol*	(Optional) Shows statistics for servers of the specified protocol: **ldap** or **radius**.

Command Default

By default, all AAA server statistics display.

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

The following table shows field descriptions for the output of the **show aaa-server** command:

Field	Description
Server Group	The server group name.
Server Protocol	The server protocol for the server group.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the system and the AAA server.
Server status	The status of the server. If the status is followed by "(admin initiated)," then the server was manually failed or reactivated using the **aaa-server active** or **aaa-server fail** command. Values are: • ACTIVE—The system will communicate with this AAA server • FAILED—The system cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated. The date and time of the last transaction appears in one of the following form: • `Last Transaction success at` *`time timezone date`* • `Last Transaction failure at` *`time timezone date`* • `Last Transaction at Unknown`, if the device has not yet communicated with the server.

Field	Description
Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.
Number of authentication requests	The number of authentication requests sent by the system. This value does not include retransmissions after a timeout.
Number of authorization requests	The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic, or for WebVPN and IPsec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout.
Number of accounting requests	The number of accounting requests. This value does not include retransmissions after a timeout.
Number of retransmissions	The number of times a message was retransmitted after an internal timeout. This value applies only to RADIUS servers (UDP).
Number of accepts	The number of successful authentication requests.
Number of rejects	The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.
Number of challenges	The number of times the AAA server required additional information from the user after receiving the initial username and password information.
Number of malformed responses	This value is not meaningful.
Number of bad authenticators	This value only applies to RADIUS. The number of times that the “authenticator” string in the RADIUS packet is corrupted (rare), or the shared secret key on the system does not match the one on the RADIUS server. To fix this problem, enter the correct server key.
Number of timeouts	The number of times the system has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.
Number of unrecognized responses	The number of times that the system received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server was corrupted, which is rare.

Examples

The following example shows how to display the AAA statistics for a specific server in a group:

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
```

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

Related Commands

Commands	Description
clear aaa-server statistics	Clears AAA server statistics.

show access-control-config

To display summary information about your access control policy, use the **show access-control-config** command.

show access-control-config

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command provides a summary explanation of your Access Control Policy, including the characteristics of each access control rule. The output shows the name and description of the Access Control Policy, its default action, Security Intelligence policies, and information about the access control rule sets and each access control rule. It also shows the name of referenced SSL, network analysis, intrusion, and file policies; intrusion variable set data; logging settings; and other advanced settings, including policy-level performance, preprocessing, and general settings.

The information includes policy-related connection information, such as source and destination port data (including type and code for ICMP entries) and the number of connections that matched each access control rule (hit counts).

The information also shows the HTML used for the block and interactive block actions for URL filtering.

If you are using device manager (the local manager), unsupported features will either show their default settings or they will be empty. If you are using management center, you can adjust any of these settings using the manager. You cannot configure any of the rules or options shown in this output using the CLI; you must use the manager.

Examples

The following example shows the access control configuration for a device managed using device manager, the local manager.

```
> show access-control-config

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

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

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
```

```
Logging Configuration     : Disabled
    DC                    : Disabled

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

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

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

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

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

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

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

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

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  Do not retry URL cache miss lookup  : No
  Inspect Traffic During Apply        : Yes
Network Analysis and Intrusion Policies
  Initial Intrusion Policy            : Balanced Security and Connectivity
  Initial Variable Set                : Default-Set
  Default Network Analysis Policy     : Balanced Security and Connectivity
Files and Malware Settings
  File Type Inspect Limit             : 1460
  Cloud Lookup Timeout                : 2
  Minimum File Capture Size           : 6144
  Maximum File Capture Size           : 1048576
  Min Dynamic Analysis Size           : 15360
  Max Dynamic Analysis Size           : 2097152
  Malware Detection Limit             : 10485760
Transport/Network Layer Preprocessor Settings
  Detection Settings
```

```
    Ignore VLAN Tracking Connections  : No
  Maximum Active Responses            : No Maximum
  Minimum Response Seconds            : No Minimum
  Session Termination Log Threshold   : 1048576
Detection Enhancement Settings
  Adaptive Profile                    : Disabled
Performance Settings
  Event Queue
    Maximum Queued Events             : 5
    Disable Reassembled Content Checks: False
  Performance Statistics
    Sample time (seconds)             : 300
    Minimum number of packets         : 10000
    Summary                           : False
    Log Session/Protocol Distribution : False
  Regular Expression Limits
    Match Recursion Limit             : Default
    Match Limit                       : Default
  Rule Processing Configuration
    Logged Events                     : 5
    Maximum Queued Events             : 8
    Events Ordered By                 : Content Length
Intelligent Application Bypass Settings
    State                                        : Off
Latency-Based Performance Settings
  Packet Handling                     : Disabled

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

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

Related Commands

Command	Description
show access-list	Shows the contents of Access Control Lists (ACLs).

show access-list

To display the rules and hit counters for an access list, use the **show access-list** command.

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

Syntax Description

id	(Optional) The name of an existing access list, to limit the view to this one access list.
ip_address	(Optional) The source IPv4 or IPv6 address, to limit the view to rules with this address.
brief	(Optional) Displays the access list identifiers, the hit count, and the time stamp of the last rule hit, all in hexadecimal format.
numeric	(Optional.) If you specify an ACL name, displays ports as numbers instead of names. For example, 80 instead of www.
element-count	(Optional.) Displays the total number of access control entries in all access lists defined on the system.

Command History

Release	Modification
6.1	This command was introduced.
6.6	The **numeric** and **element-count** keywords were added.
7.1	The **element-count** output includes the breakdown of object groups if object-group search is enabled.

Usage Guidelines

The system structures some elements of the Access Control Policy as advanced access control list (ACL) entries. When possible, access control rules that block traffic based on layer 3 criteria become deny rules in the ACL. You might also see trust ACL rules that align with trust access control rules.

But if an access control rule requires inspection, even if the rule action is block, the ACL entry actually permits the traffic. This permitted traffic is then passed to the inspection engines, such as snort, which can ultimately block unwanted traffic.

Thus, there is not a one-to-one relationship between the low-level ACL rules shown with **show access-list** and the Access Control Policy rules for the device. The advanced ACL allows the system to make early drop or trust decisions on traffic, so connections that do not need inspection can be passed or dropped as quickly as possible.

Note If your goal is to view hit count information for access control and prefilter rules, use the **show rule hits** command instead of this one.

ACLs can also be used for other things, such as route maps and match criteria for service policies. Standard and extended ACLs are used for these purposes.

You can display multiple access lists at one time by entering the access list identifiers in one command.

You can specify the **brief** keyword to display access list hit count, identifiers, and timestamp information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in three columns, and they are the same identifiers used in syslogs 106023 and 106100.

If an access list has been changed recently, the list is excluded from the output. A message will indicate when this happens.

Note The output shows how many elements are in the ACL. This number is not necessarily the same as the number of access control entries (ACE) in the ACL. The system might create extra elements when you use network objects with address ranges, for example, and these extra elements are not included in the output.

Clustering Guidelines

When using clustering, if traffic is received by a single unit, the other units may still show a hit count for the ACL due to the clustering director logic. This is an expected behavior. Because the unit that did not receive any packets directly from the client may receive forwarded packets over the cluster control link for an owner request, the unit may check the ACL before sending the packet back to the receiving unit. As a result, the ACL hit count will be increased even though the unit did not pass the traffic.

Examples

The following is sample output from the **show access-list** command and shows the advanced access list generated for the Access Control Policy when using device manager (the local or "on box" manager). The remarks are system-generated to help you understand the access control entries (ACEs). Note that the remarks give you the name of the related rule; ACEs generated from the rule follow. These remarks are highlighted in the example below.

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xc5a178c1
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any
```

```
rule-id 268435458 event-log both (hitcnt=0) 0xdbc1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x3571535c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x118ef4b4
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 28 advanced trust ip ifc inside1_6 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xc6bfe6b7
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x5fe085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xe415bb76
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf9bfd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xf08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x952c7254
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xfc38a46f
access-list NGFW_ONBOX_ACL line 42 advanced trust ip ifc inside1_8 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x3f878e23
access-list NGFW_ONBOX_ACL line 43 advanced trust ip ifc inside1_8 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x48e852ce
access-list NGFW_ONBOX_ACL line 44 advanced trust ip ifc inside1_8 any ifc inside1_7 any
```

```
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
access-list NGFW_ONBOX_ACL line 45 remark rule-id 268435457: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 46 remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xea5bdd6e
access-list NGFW_ONBOX_ACL line 48 advanced trust ip ifc inside1_3 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xd7461ffc
access-list NGFW_ONBOX_ACL line 49 advanced trust ip ifc inside1_4 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x6e13508e
access-list NGFW_ONBOX_ACL line 50 advanced trust ip ifc inside1_5 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xfe1fcdd6
access-list NGFW_ONBOX_ACL line 51 advanced trust ip ifc inside1_6 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xa4dba9a8
access-list NGFW_ONBOX_ACL line 52 advanced trust ip ifc inside1_7 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 53 advanced trust ip ifc inside1_8 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xc3c3fafb
access-list NGFW_ONBOX_ACL line 54 remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 55 remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL line 56 advanced deny ip any any rule-id 1 (hitcnt=0)
0x84953cae
>
```

The following examples show brief information about the specified access policy in hexadecimal format (ACEs in which the hitcount is not zero). The first two columns display identifiers in hexadecimal format, the third column lists the hit count, and the fourth column displays the timestamp value, also in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. The timestamp value reports the time of the last hit. If the hit count is zero, no information is displayed.

The following is sample output from the **show access-list brief** command when Telnet traffic is passed:

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

The following is sample output from the **show access-list brief** command when SSH traffic is passed:

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

The following example shows the element count, which is the total number of access control entries for all access lists defined on the system. For access lists that are assigned as access groups, to control access globally or on an interface, you can reduce the element count by enabling object group search, which is represented by the **object-group-search access-control** command in the running configuration. When object group search is enabled, network objects are used in the access control entries; otherwise, the objects are expanded into the individual IP addresses contained in the objects and separate entries are written for each source/destination address pair. Thus, a single rule that uses a source network object with 5 IP addresses, and a destination object with 6 addresses, would expand into 5 * 6 entries, 30 elements rather than one. The higher the element count, the larger the access lists, which can potentially impact performance.

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

Starting with 7.1, if you enable object-group search, additional information is presented about the number of object groups in the rules (OBJGRP), including the split between source (SRC OBJ) and destination (DST OBJ) objects, and the added and deleted groups.

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

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

Related Commands

Command	Description
clear access-list	Clears an access list counter.
show running-config access-list	Displays the current running access-list configuration.

show alarm settings

To display the configuration for each type of alarm in the ISA 3000, use the **show alarm settings** command.

show alarm settings

Command History

Release	Modification
6.3	This command was introduced.

Examples

The following is a sample output from the **show alarm settings** command:

```
> show alarm settings

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

Related Commands

Command	Description
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.
show environment alarm-contact	Displays the status of the input alarm contacts.
show facility-alarm	Displays status information for triggered alarms.

show allocate-core

To display information about how CPU cores are allocated, use the **show allocate-core** command.

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

Syntax Description

lina-cpu-percentage	Shows the percentage of CPU cores allocated to the Lina process. The remaining cores are allocated to the Snort process.
lina-mem-percentage	Shows the percentage of system memory allocated to the Lina process. The remaining memory is allocated to the Snort process.
profile	Shows the core allocation profile currently operating on the device.
state	Shows whether the core allocation process is enabled or disabled.

Command History

Release	Modification
7.3	This command was added.

Usage Guidelines

You can assign CPU core allocation profiles from the management software. Use this command to view and verify the profile running on a device. Possible profiles are:

- default—The default scheme of core allocation for the Lina and Snort processes. The exact allocation differs based on hardware platform. Use the other options to determine the percentages.
- ips-heavy—Allocates more CPU to Snort for the IPS-heavy use case. The allocation is 30% Lina, 70% Snort.
- vpn-heavy-prefilter-fastpath—Allocates more CPU to Lina for the VPN-heavy use case when you also configure a prefilter policy to fastpath VPN traffic. The allocation is 90% Lina, 10% Snort.
- vpn-heavy-with-inspection—Allocates more CPU to Lina for the VPN-heavy use case when you do not configure a prefilter policy to fastpath VPN traffic, but instead have the traffic inspected in the access-control policy. The allocation is 60% Lina, 40% Snort.

Example

The following example shows the Lina CPU and memory percentages, the profile, and the core allocation state.

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

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

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

Core allocation profile is set to : default
```

```
> show allocate-core state
Core allocation is disabled
```

show app-agent heartbeat

To display the status of the app-agent, use the **show app-agent heartbeat** command.

show app-agent heartbeat

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The app-agent heartbeat communication channel serves the purpose of monitoring the health of the link between FXOS chassis supervisor and threat defense application agent. This is used if you configure hardware bypass on Firepower 4100 or 9300 series devices. It is not used with other device models running threat defense software.

Use the **show app-agent heartbeat** command to view status on the app-agent heartbeat communication channel.

Examples

The following example shows the app-agent heartbeat status.

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

Related Commands

Command	Description
app-agent	Configures the app-agent for Hardware Bypass.

show arp

To view the ARP table, use the **show arp** command.

show arp

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.”

The ARP table can include entries for internal interfaces, such as nlp_int_tap, which are used for system communications.

Examples

The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

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

Related Commands

Command	Description
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config all arp	Shows the current configuration of the ARP timeout.

show arp-inspection

To view the ARP inspection setting for each interface, use the **show arp-inspection** command.

show arp-inspection

Command History

Release	Modification
6.1	This command was added.
6.2	Support for routed mode was added.

Examples

The following is sample output from the **show arp-inspection** command:

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

The miss column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

Related Commands

Command	Description
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config all arp	Shows the current configuration of the ARP timeout.

show arp statistics

To view ARP statistics, use the **show arp statistics** command.

show arp statistics

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

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

The following table explains each field.

Table 1: show arp statistics Fields (continued)

Field	Description
Number of ARP entries	The total number of ARP table entries.
Dropped blocks in ARP	The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.
Maximum queued blocks	The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all interfaces that were from the same IP address as that of an interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the device as part of the ARP-Defense mechanism.
Total ARP retries	The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.

Field	Description
Unresolved hosts	The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.
Maximum unresolved hosts	The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the device booted up.

Related Commands

Command	Description
clear arp statistics	Clears ARP statistics.
show arp	Shows the ARP table.
show running-config all arp	Shows the current configuration of the ARP timeout.

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.

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

Syntax Description

number	(Optional) Specifies the AS path access list number. Valid values are between 1 and 500.

Command Default

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

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

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

 AS path access list 2
```

show asp cluster counter

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

show asp cluster counter

Command History

Release	Modification
6.1	This command was introduced.

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:

```
> 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. It is only available for a threat defense virtual device in the hybrid poll/interrupt mode.

show asp dispatch

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

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

Last clearing of asp dispatch: Never

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

show asp drop

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

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

Command History

Release	Modification
6.1	This command was introduced.

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. 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 information on the possible drop reasons, see the Show ASP Drop Command Usage document at http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html.

Examples

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

```
> show asp drop

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

Last clearing: Never

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

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

show asp event

To debug the data path or control path event queues, use the **show asp event** command.

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

Syntax Description

dp-cp	Show events sent from the ASP data-path to the control plane.
cp-dp	Show events sent from the control plane to the ASP data-path.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show asp event** command shows the contents of the data path and control path, which might help you troubleshoot a problem. 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:

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

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

show asp inspect-dp ack-passthrough

To show statistics related to empty ACK packets that bypass Snort inspection, use the **show asp inspect-dp ack-passthrough** command.

show asp inspect-dp ack-passthrough

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **clear asp inspect-dp ack-passthrough** command to reset these statistics.

Example

The following is example output. Information includes whether ACK passthrough is enabled, and the following statistics:

- ACK packets bypassed—The number of empty ACK packets that were not forwarded to Snort for inspection.
- Meta ACK sent—The number of empty ACKs piggybacked on subsequent data packets that were sent to Snort. This number can be less than the number of packets bypassed, because if a subsequent data packet for the same direction has an ACK with a higher sequence number, the empty ACK information that was saved earlier is not needed and is not included.

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

Current running state: Enabled

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

show asp inspect-dp egress-optimization

Displays statistics about egress optimization, a feature that enhances performance. Use this command on the advice of Cisco TAC.

show asp inspect-dp egress optimization

Command History

Release	Modification
6.4	This command was introduced.

Usage Guidelines

The **show asp inspect-dp egress-optimization** command displays information about flows eligible for egress optimization, a feature that enhances performance. The output displays the following information:

- Current running state: Whether egress optimization is enabled or disabled.
- Flow (a *flow* consists of one or more *packets*):
  - Current: Number of flows that are currently eligible for egress optimization processing.
  - Maximum: Total number of egress-optimization eligible flows since the last time inspection engine was restarted or egress optimization statistics were cleared.
- Packet:
  - Processed: Total number of packets processed.
  - Excepted: Number of packets that were initially determined to be eligible for egress optimization but later determined to be ineligible for egress optimization.

Examples

The following is sample output from the **show asp inspect-dp egress-optimization** command.

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

Related Commands

Commands	Description
clear asp inspect-dp egress-optimization	Clears egress optimization statistics.

Commands	Description
show conn state egress_optimization	Displays information about flows eligible for egress optimization. Use this command on the advice of Cisco TAC.

show asp inspect-dp snapshot

To view the snapshot of a PDTS (data plane transmit/receive queues to snort) ring, use the **show asp inspect-dp snapshot** command.

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

Syntax Description

config	Displays the global configuration for PDTS snapshots.
instance *instance_id*	Displays snapshot for the specified PDTS consumer instance ID. Values are from 0-2147483647.
queue *queue_id*	Displays the snapshot for the specified data path transmit queue ID of a PDTS ring. Values are from 0-2147483647.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show asp inspect-dp snapshot** command displays the global configurations of the PDTS ring snapshot feature. The output displays the following information:

- Max snapshots: The maximum number of auto snapshots allowed.
- Current in use: The number of snapshots that have been stored so far.
- Interval: The time interval value specifies how long two snapshots on the same PDTS ring are allowed
- Auto Snapshot: Show if auto PDTS snapshot feature is enabled or disabled

Examples

The following is sample output from the **show asp inspect-dp snapshot config** command.

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

The following is sample output from the **show asp inspect-dp snapshot instance** command.

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

show asp inspect-dp snort

To display the status of all snort instances, use the **show asp inspect-dp snort** command.

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

Syntax Description

instance *instance_id*	Displays the status of the specific snort instance. Values for are from 0-2147483647.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays the status of all snort instances. The output displays the following information:

- Id: SNORT instance ID.
- PID: Snort instance process ID.
- CPU-Usage: CPU usage for the snort instance ID. Printed in total, and user/sys. **Note:** This field is not shown for the Firepower 2100 series.
- Conns: Number of connections currently held by the snort instance.
- Segs/Pkts: Number of segments or say packets currently processed by the snort instance.
- Status: The status of the snort instance.

Examples

The following is sample output from the **show asp inspect-dp snort** command.

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

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

The following is sample output from the **show asp inspect-dp snort** command on the Firepower 2100.

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid   Conns      Segs/Pkts  Status
-- ----- ---------- ---------- ----------
```

```
0  30080  40          0        READY
1  30081  14          0        READY
2  30079  20          0        READY
```

show asp inspect-dp snort counters

To display the PDTS related raw counters for snort instances, use the **show asp inspect-dp snort counters** command.

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

Syntax Description

instance *instance_id*	Displays the counters for the specific snort instance. Values are from 0-2147483647.
queues	Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.
rate	It takes the counters snapshot for 5 seconds, averaged to one sec, and shows the rate of the counter changes.
debug	It displays certain debug counters not otherwise displayed.
zeros	All counters including zero counters will be displayed.

Command Default

If no instance is specified, all instances are displayed.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays the PDTS related raw counters for snort instances. The output displays the following information:

- Id: Snort instance ID. “All” means all snort instances aggregated.
- QId: Lina transmit queue ID. It corresponds to the number of Lina threads.“All” means all the queues are aggregated.
- Type: Type of the counter. Data counter, error counter, debug counters, etc.
- Name: Name of the counter.
- Value: Human readable value of the counter.
- Raw-Value: Raw value of the counter.

Counter Names:

- Tx Bytes: Number of bytes Lina sent to the snort instance.
- Tx Segs: Number of frames/segments Lina sent to the snort instance.
- Rx Bytes: Number of bytes Lina received from the snort instance.
- Rx Segs: Number of frames/segments Lina received from the snort instance.
- NewConns: Number of connections sent to the snort instance.

- RxQ-Wakeup
- TxQ-Wakeup
- TxQ-LB-Dynamic: Number of times the PDTS dynamic load balancing kicked in.
- TxQ-Data-Hi-Thresh: Number of times the High threshold limit on Lina's transmit queue is hit.
- RxQ-Full: Number of times the Lina's receive queue gets full.
- TxQ-Full: Number of times the Lina's transmit queue gets full.
- TxQ-Data-Limit: Number of times the data limit on Lina's transmit queue is hit.
- TxQ-LB-Failed: Number of times the PDTS dynamic load balancing failed.
- TxQ-Unavail: Number of times Lina's transmit queue is unavailable.
- TxQ-Not-Ready: Number of times Lina's transmit queue is not ready.
- TxQ-Suspended: Number of times Lina's transmit queue is suspended.
- RxQ-Unavail: Number of times Lina's receive queue is unavailable.
- RxQ-Not-Ready: Number of times Lina's receive queue is not ready.
- RxQ-Suspended: Number of times Lina's receive queue is suspended.

Examples

The following is sample output from the **show asp inspect-dp snort counters** command.

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

show asp inspect-dp snort counters summary

To display the PDTS related counters for snort instances, use the **show asp inspect-dp snort counters summary** command. Counters are aggregated to each instance.

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

Syntax Description

instance *instance_id*	Displays the counters for the specific snort instance. Values are from 0-2147483647.
queues	Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.
rate	Displays the one second average increase in the counter. Currently the one sec average is based on the delta increase between the last and current invocation of the command. This will change such that the delta increase is based on a 5 second rolling average, sampled once a second.

Command Default

If no instance is specified, all instances are displayed.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays the PDTS related counters for snort instances. The output displays the following information:

- Id: Snort instance ID. “All” means all snort instances aggregated.
- QId: Lina transmit queue ID. It corresponds to the number of Lina threads.“All” means all the queues are aggregated.
- TxBytes: Total number of bytes Lina sent to the snort instance.
- TxFrames: Total number of frames/segments Lina sent to the snort instance.
- RxBytes: Total number of bytes Lina received from the snort instance.
- RxFrames: Total number of frames/segments Lina received from the snort instance.
- Conns: Total number of connections handled by the snort instance.

Examples

The following is sample output from the **show asp inspect-dp snort counters summary** command.

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

show asp inspect-dp snort queues

To display the queue information for all snort instances (processes) aggregating all queues to the same instance, use the **show asp inspect-dp snort queues** command.

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

Syntax Description

instance *instance_id*	Displays the queues for the specific snort instance. Values are from 0-2147483647.
detail	Displays the queues information in detail. Each producer queue for the instance is displayed separately. Queue information of an instance will not be aggregated.
debug	Extra debug information will also be displayed.

Command Default

If no instance is specified, all instances are displayed.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays the queue information for all snort instances (processes) aggregating all queue to the same instance, The output displays the following information:

- Id: Snort instance ID. “All” means all snort instances aggregated.
- QId: Lina transmit queue ID. It corresponds to the number of Lina threads.“All” means all the queues are aggregated.
- Rx Queue: Lina’s receive queue. “Used” shows amount of data, “util” is the queue utilization rate, and “state” shows the shared memory state.
- TxQ: Lina’s transmit queue. “Used” shows amount of data, “util” is the queueutilization rate, and “state” shows the shared memory state.

Counters:

- RxQ-Size: Lina’s receive queue size.
- TxQ-Size: Lina’s transmit queue size.
- TxQ-Data-Limit: The data limit of transmit queue. Once beyond this threshold, data packetswill be dropped. The percentage shows the threshold value on the transmit queue.
- TxQ-Data-Hi-Thresh: The High threshold of transmit queue. Once beyond this threshold, PDTS dynamic load balancing will kick in to try balancing the flows to other snort instances.

Examples

The following is sample output from the **show asp inspect-dp snort queues** command.

```
> show asp inspect-dp snort counters summary instance 2
```

```
SNORT Inspect Instance Queue Configuration

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

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

show asp inspect-dp snort queue-exhaustion

To display the automatic snapshots of when a snort queue exhaustion occurs, use the **show asp inspect-dp snort queue-exhaustion** command.

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

Syntax Description

snapshot *snapshot_id*	This option specifies a particular snapshot to print the queue exhaustion information. Values are between 1 and 24.
export *location*	The contents of a snapshot are exported into a pcap file at the specified location, for off-box analysis.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show asp inspect-dp snort queue-exhaustion** command displays the contents of the snapshots taken when snort queues are exhausted. It shows the contents of a selected snapshot. The output is similar to the output of **show capture** command.

Examples

The following is sample output from the **show asp inspect-dp snort queue-exhaustion** command.

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

show asp load-balance

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

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

Syntax Description

detail	(Optional) Shows detailed information about hash buckets used in the samples.

Command History

Release	Modification
6.1	This command was introduced.

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.

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                    ASP load balancer queue sizes
  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
      |                          #
      |   # #                    # #           #
      |   # #                    # #           #
      +---------+---------+---------+---------+---------+---------+----
                10        20        30        40        50        60
                          # of queued jobs per queue
```

Related Commands

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

show asp multiprocessor accelerated- features

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

show asp multiprocessor accelerated-features

Command History

Release	Modification
6.1	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:

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

show asp overhead

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

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 History

Release	Modification
6.1	This command was introduced.

Examples

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

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

show asp packet-profile

To display the counters for how many packets were fastpathed by a prefilter policy, offloaded as a large flow, and fully evaluated by access control (Snort), use the **show asp packet-profile** command.

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

Syntax Description

data-path	Displays the counters for the data plane packet profiles.
offload	Displays the counters for the hardware offload packet profiles.
snort	Displays the counters for the snort packet profiles.

Command Default

If no instance is specified, all instances are displayed.

Command History

Release	Modification
6.5	This command was introduced.

Usage Guidelines

Each packet traversing a threat defense device goes through various stages of processing depending on the access policies configured, the Snort verdicts, and hardware capabilities like flow offload support.

Global counters are used to track these statistics and are updated at the end of each session. These global counters are collected and represented in the form of a histogram. At any given point the histogram displays the cumulative packet counters processed by the system since device boot up time or the last restart.

Examples

The following is sample output from the **show asp packet-profile** command.

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

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

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

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

                Packets         :    Connections
                [0-3]           :              0
                [4-7]           :           6202
                [8-15]          :          10950
                [16-31]         :           2487
```

```
        [32-63]         :                   85
        [64-127]        :                    0
        [128-255]       :                    0
        [256-511]       :                    0
        [512-1023]      :                    0
        [1024 and above]:                    0

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

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

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

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

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

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

show asp rule-engine

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

show asp rule-engine

Command History

Release	Modification
7.1	This command was introduced.

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.

```
> show asp rule-engine

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

Module    |  Insert   |  Remove   |  Current   |

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

show asp table arp

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

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.

Command History

Release	Modification
6.1	This command was introduced.

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. 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 arp** command:

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

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.

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

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.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show asp table classify** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. 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:

```
> 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
```

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.

show asp table cluster chash-table

Command History

Release	Modification
6.1	This command was introduced.

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. 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:

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

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

Related Commands

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

show asp table interfaces

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

show asp table interfaces

Command History

Release	Modification
6.1	This command was introduced.

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. 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:

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

show asp table network-service

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

show asp table network-service

Command History

Release	Modification
7.1	This command was introduced.

Example

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

```
> show asp table network-service
Per-Context Category NSG:
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

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

show asp table routing

To debug the accelerated security path routing tables, use the **show asp table routing** command. This command supports IPv4 and IPv6 addresses.

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

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 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.
[**vrf** *name* | **all**]	If you enable virtual routing and forwarding (VRF), also known as virtual routers, you can limit the view to a specific virtual router using the **vrf** *name* keyword. If you want to see the routing tables for all virtual routers, include the **all** keyword. If you include neither of these VRF-related keywords, the command shows the routing table for the global VRF virtual router.

Command History

Release	Modification
6.1	This command was introduced.
6.6	The [**vrf** *name* | **all**] keywords were 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. 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.

Examples

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

```
> 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
```

The following example shows the routing table for the virtual router named alpha.

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

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.

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

Syntax Description

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

Command History

Release	Modification
6.1	This command was introduced.

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. 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:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
     checksum errors 0
  Sent:
     total 0
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
```

```
SSL Close: 117
SSL Server: 58
SSL Server Verify: 0
SSL Client: 0
```

TCP/UDP 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 device, 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.instance

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.

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

Syntax Description

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

Command History

Release	Modification
6.1	This command was introduced.

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. 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:

```
> 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:

```
> 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. When the persistent IPsec tunneled flows feature is enabled, the flags will include the PRESERVE flag.

```
> show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
```

```
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

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

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.

show asp table zone

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show asp table zone** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. 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. In this example, the zone named is-154 is actually an inline set, not a traffic zone.

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

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

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

Related Commands

Command	Description
show inline-set	Shows the inline sets.
show zone	Shows the traffic zones.

show audit-log

To display the system audit log, use the **show audit-log** command.

show audit-log

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays the audit log in reverse chronological order; the most recent audit log events are listed first.

Events can include system updates, permission problems, configuration changes, and policy applications. The information is available for devices remotely managed by management center only. The audit log is empty for locally managed systems.

Examples

The following example shows the audit log.

```
> show audit-log
Audit Log Output:
 time                   :  1476223151 (Tue Oct 11 21:59:11 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Clam update synchronization
from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222646 (Tue Oct 11 21:50:46 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply AMP Dynamic Analysis C
onfiguration from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222564 (Tue Oct 11 21:49:24 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply Initial_Health_Policy
2016-10-11 18:54:59 from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222563 (Tue Oct 11 21:49:23 2016)
 event_type             :  notify
 subsystem              :  Health > Health Policy > Apply > Initial_Health_Policy 20
```

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