sa - show a

sftunnel-status

要查看设备和管理 管理中心之间的连接（隧道）状态，请使用 **sftunnel-status** 命令。

sftunnel-status

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **sftunnel-status** 命令查看设备和管理 管理中心之间的连接状态。如果使用的是本地管理器 设备管理器，则此命令不提供任何信息。

状态信息包括以下会话：

- SFTUNNEL 状态 - 建立连接的时间以及连接中使用的管理接口的相关信息。
- RUN STATUS - IP 地址、加密和注册状态信息。
- 对等体信息 - 有关 管理中心 及其与此设备的连接的信息。本节还包括可能在系统之间传输的各种服务的几种消息类型的统计信息块，包括身份、运行状况事件、RPC、NTP、IDS、恶意软件查找、CSM_CCM（用于配置设备）、EStreamer、UE 通道和 FSTREAM。
- RPC 状态:

示例

以下是 **sftunnel-status** 命令的输出示例。

```
> 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

命令	Description
configure manager add	添加远程管理器 管理中心。

sftunnel-status-brief

要查看设备和管理 管理中心之间的连接（隧道）的简要状态，请使用 **sftunnel-status-brief** 命令。

sftunnel-status-brief

Command History

版本	修改
6.7	引入了此命令。

使用指南

输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

示例

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> 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
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> 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

命令	Description
sftunnel-status	显示管理隧道状态的详细信息。

show aaa-server

要显示 AAA 服务器的统计信息，请使用 **show aaa-server** 命令。

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

Syntax Description

groupname	（可选）显示组中服务器的统计信息。
host *hostname*	（可选）显示组中特定服务器的统计信息。
LOCAL	（可选）显示 LOCAL 用户数据库的统计信息。
protocol *protocol*	（可选）显示指定协议的服务器的统计信息： **ldap** 或 **radius**。

Command Default

默认显示所有 AAA 服务器统计信息。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

下表显示了 **show aaa-server** 命令的输出的字段描述：

字段	Description
Server Group	服务器组名称。
Server Protocol	服务器组的服务器协议。
Server Address	AAA 服务器的 IP 地址。
Server port	系统和 AAA 服务器使用的通信端口。
Server status	服务器的状态。如果状态后接“(admin initiated)”，则表示服务器是使用 **aaa-server active** 或 **aaa-server fail** 命令手动重新激活或设置成失败的。其值如下： • ACTIVE - 系统将与此 AAA 服务器通信。 • FAILED - 系统无法与 AAA 服务器通信。根据配置的策略，处于此状态的服务器将保持该状态一段时间，然后重新激活。 最后一个事务的日期和时间使用以下形式之一显示： • `Last Transaction success at time timezone date` • `Last Transaction failure at time timezone date` • 如果设备尚未与服务器通信，则`Last Transaction at Unknown`。

字段	Description
Number of pending requests	仍在进行中的请求数。
Average round trip time	完成与服务器的事务所需的平均时间。
Number of authentication requests	系统发送的身份验证请求数。此值不包括在超时之后的重新传输。
Number of authorization requests	授权请求数。此值是指源于以下项的授权请求：命令授权、通过机箱流量的授权、为隧道组启用的 WebVPN 和 IPsec 授权功能。此值不包括在超时之后的重新传输。
Number of accounting requests	记账请求数。此值不包括在超时之后的重新传输。
Number of retransmissions	在内部超时后重新传输消息的次数。此值仅适用于RADIUS服务器(UDP)。
Number of accepts	成功的身份验证请求数。
Number of rejects	拒绝的请求数。此值包括错误情况以及来自AAA服务器的真实凭证拒绝。
Number of challenges	AAA 服务器在收到初始用户名和密码信息后要求提供其他信息的次数。
Number of malformed responses	此值没有意义。
Number of bad authenticators	此值仅适用于 RADIUS。 RADIUS 数据包中的“authenticator”字符串损坏（罕见）或系统上的共享密钥与RADIUS服务器上的密钥不匹配的次数。要解决此问题，请输入正确的服务器密钥。
Number of timeouts	系统检测到 AAA 服务器未响应或行为错误并已宣布其离线的次数。
Number of unrecognized responses	系统从 AAA 服务器收到它无法标识或支持的响应的次数。例如，来自服务器的 RADIUS 数据包代码是“access-accept”、“access-reject”、“access-challenge”或“accounting-response”以外的未知类型。通常情况下，这意味着来自服务器的RADIUS响应数据包已损坏，但这种情况很少出现。

示例

以下示例展示如何显示组中特定服务器的 AAA 统计信息：

```
> 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

命令	Description
clear aaa-server statistics	清除 AAA 服务器统计信息。

show access-control-config

要显示有关访问控制策略的摘要信息，请使用 **show access-control-config** 命令。

show access-control-config

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令提供访问控制策略的摘要说明，包括每个访问控制规则的特征。输出显示访问控制策略的名称和说明、其默认操作、安全情报策略以及有关访问控制规则集和每个访问控制规则的信息。也显示引用的 SSL 的名称、网络分析、入侵和文件策略名称；入侵变量集数据；日志记录设置；以及其他高级设置，包括政策级别性能、预处理和常规设置。

信息包括策略相关的连接信息，例如源端口和目标端口数据（包括 ICMP 条目的类型和代码）以及与每条访问控制规则匹配的连接数（命中次数）。

该信息还显示用于 URL 过滤的阻止和交互式阻止操作的 HTML。

如果您使用 设备管理器（本地管理器），则不受支持的功能将显示其默认设置或为空。如果您使用的是 管理中心，则可以使用管理器调整任何这些设置。您无法使用 CLI 配置此输出中显示的任何规则或选项；您必须使用管理器。

示例

以下示例显示使用本地管理器 设备管理器管理的设备的访问控制配置。

```
> 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

命令	Description
show access-list	显示访问控制列表 (ACL) 的内容。

show access-list

要显示访问列表的规则和命中计数器，请使用 **show access-list** 命令。

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

Syntax Description

ID	（可选）现有访问列表的名称，以将视图限制为此访问列表。
ip_address	（可选）源 IPv4 或 IPv6 地址，以将视图限制为具有此地址的规则。
brief	（可选）显示访问列表标识符、命中计数以及最后规则命中的时间戳，全部采用十六进制格式。
numeric	（可选。）如果指定ACL名称，则将端口显示为编号而不是名称。例如，80 而不是 www。
element-count	（可选。）显示系统上定义的所有访问列表中的访问控制条目总数。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 **numeric** 和 **element-count** 关键字。
7.1	如果启用了对象组搜索，则 **element-count** 输出包括对象组的细分。

使用指南

系统将访问控制策略的某些元素构建为高级访问控制列表 (ACL) 条目。如果可能，根据第 3 层条件阻止流量的访问控制规则将成为ACL中的拒绝规则。您可能还会看到与信任访问控制规则一致的信任 ACL 规则。

但是，如果访问控制规则需要检查，即使规则操作是阻止，ACL 条目实际上也允许流量。然后，这些允许的流量将传递到检测引擎（例如 snort），最终会阻止不需要的流量。

因此， **show access-list** 显示的低级 ACL 规则与设备的访问控制策略规则之间没有一对一的关系。高级 ACL 允许系统及早对流量做出丢弃或信任决策，因此可以尽快通过或丢弃不需要检查的连接。

注释 如果您的目标是查看访问控制和预过滤器规则的命中计数信息，请使用 **show rule hits** 命令而不是此命令。

ACL 还可用于其他用途，例如路由地图和服务策略的匹配条件。标准和扩展 ACL 用于这些目的。

您可以在一个命令中输入访问列表标识符，一次显示多个访问列表。

您可以指定**brief**关键字，以十六进制格式显示访问列表命中数、标识符和时间戳信息。以十六进制格式显示配置标识符分三列显示，与系统日志 106023 和 106100 中使用的标识符相同。

如果访问列表最近已更改，则该列表将从输出中排除。系统将显示一条消息，指示何时发生这种情况。

注释 输出显示 ACL 中有多少个元素。此数量不一定与 ACL 中的访问控制条目 (ACE) 数量相同。例如，当您使用具有地址范围的网络对象时，系统可能会创建额外的元素，而这些额外的元素不包含在输出中。

集群准则

使用集群时，由于集群管理逻辑的作用，如果其中一台设备收到流量，其他设备仍可能显示ACL的命中计数。这是预期行为。由于未直接从客户端收到任何数据包的设备可能会收到通过所有者请求的集群控制链路转发的数据包，因此，该设备在将数据包发回接收设备之前，可能会检查 ACL。因此，即使设备未传递流量，ACL 命中计数也会增加。

示例

以下是 **show access-list** 命令的输出示例，显示了使用 设备管理器 （本地或“on box”管理器时）为访问控制策略生成的高级访问列表。这些备注是系统生成的，可帮助您了解访问控制条目 (ACE)。请注意，备注为您提供相关规则的名称；根据规则生成的 ACE 如下。这些备注在下面的示例中突出显示。

```
> 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
>
```

以下示例以十六进制格式显示指定访问策略的简短信息（命中计数不是零的 ACE）。前两列以十六进制格式显示标识符，第三列显示命中计数，第四列显示时间戳值（也是十六进制格式）。命中计数值代表流量命中规则的次数。时间戳值报告最后一次命中的时间。如果命中计数为零，则不会显示任何信息。

以下是当 Telnet 流量通过时 **show access-list brief** 命令的输出示例：。

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

以下是当 SSH 流量通过时 **show access-list brief** 命令的输出示例：。

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

以下示例显示元素计数，即系统上定义的所有访问列表的访问控制条目总数。对于分配为访问组的访问列表，要全局控制访问或在接口上控制访问，可以通过启用对象组搜索来减少元素计数，这在运行配置中由 **object-group-search access-control** 命令表示。启用对象组搜索时，将在访问控制条目中使用网络对象；否则，对象将扩展为对象中包含的单个 IP 地址，并为每个源/目标地址对写入单独的条目。因此，使用具有 5 个 IP 地址的源网络对象和具有 6 个地址的目标对象的单个规则将扩展为 5 * 6 个条目，而不是一个元素。元素计数越高，访问列表越大，这可能会影响性能。

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

从 7.1 开始，如果启用对象组搜索，则会显示有关规则 (OBJGRP) 中对象组数量的其他信息，包括源 (SRC OBJ) 和目标 (DST OBJ) 对象之间的拆分，以及添加的和已删除的组。

```
> 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

命令	Description
clear access-list	清除访问列表计数器。
show running-config access-list	显示当前正在运行的访问列表配置。

show alarm settings

要显示 ISA 3000 中每种警报的配置，请使用 **show alarm settings** 命令。

show alarm settings

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show alarm settings** 命令的输出示例：

```
> 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

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show environment alarm-contact	显示输入警报触点的状态。
show facility-alarm	显示已触发警报的状态信息。

show allocate-core

要显示有关如何分配 CPU 核心的信息，请使用 **show allocate-core** 命令。

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

Syntax Description

lina-cpu-percentage	显示分配给 Lina 流程的 CPU 核心百分比。其余核心分配给 Snort 流程。
lina-mem-percentage	显示分配给 Lina 流程的系统内存百分比。剩余的内存分配给 Snort 流程。
profile	显示设备上当前运行的核心分配配置文件。
state	显示核心分配流程是已启用还是已禁用。

Command History

版本	修改
7.3	添加了此命令。

使用指南

您可以从管理软件分配CPU核心分配配置文件。使用此命令可查看和验证设备上运行的配置文件。可能的配置文件包括：

- default - Lina 和 Snort 流程的默认核心分配方案。确切的分配因硬件平台而异。使用其他选项确定百分比。
- ips-heavy - 为 IPS 为主的使用案例向 Snort 分配更多 CPU。分配比例为 Lina 30%，Snort 70%。
- vpn-heavy-prefilter-fastpath - 将预过滤器策略配置为快速路径 VPN 流量时，会为大量使用 VPN 的使用案例向 Lina 分配更多 CPU。分配比例为 Lina 90%，Snort 10%。
- vpn-heavy-with-inspection - 未将预过滤器策略配置为快速路径 VPN 流量，而是在访问控制策略中检查流量时，为 VPN 大量使用案例向 Lina 分配更多 CPU。分配比例为 Lina 60%，Snort 40%。

示例

以下示例显示 Lina CPU 和内存百分比、配置文件和核心分配状态。

```
> 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

要显示应用代理的状态，请使用 **show app-agent heartbeat** 命令。

show app-agent heartbeat

Command History

版本	修改
6.1	引入了此命令。

使用指南

应用代理心跳通信信道用于监控 FXOS 机箱管理引擎和 threat defense 应用代理之间的链路的运行状况。如果在 Firepower 4100 或 9300 系列设备上配置硬件绕行，则使用此选项。它不适用于运行 threat defense 软件的其他设备型号。

使用 **show app-agent heartbeat** 命令查看 app-agent 心跳通信信道上的状态。

示例

以下示例显示了 app-agent 心跳状态。

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

Related Commands

命令	Description
app-agent	为硬件旁路配置应用代理。

show arp

要查看 ARP 表，请使用 **show arp** 命令。

show arp

Command History

版本	修改
6.1	引入了此命令。

使用指南

显示输出会显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。静态 ARP 条目以短划线 (-) 取代时限，代理 ARP 条目则显示“别名”。

ARP 表可以包括用于系统通信的内部接口条目，例如 nlp_int_tap。

示例

以下是 **show arp** 命令的输出示例。第一个条目是时限为 2 秒的动态条目。第二个条目是静态条目，第三个条目来自代理 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

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config all arp	显示 ARP 超时的当前配置。

show arp-inspection

要查看每个接口的 ARP 检测设置，请使用 **show arp-inspection** 命令。

show arp-inspection

Command History

版本	修改
6.1	添加了此命令。
6.2	添加了对路由模式的支持。

示例

以下是 **show arp-inspection** 命令的输出示例：

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

Miss 列显示在 ARP 检查启用后要对非匹配数据包采取的默认操作（“泛洪”或“无泛洪”）。

Related Commands

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config all arp	显示 ARP 超时的当前配置。

show arp statistics

要查看 ARP 统计信息，请使用 **show arp statistics** 命令。

show arp statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show arp statistics** 命令的输出示例：

```
> 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
```

下表对每个字段进行了说明。

表 *1: show arp statistics* 字段（续）

字段	Description
Number of ARP entries	ARP 表条目的总数。
Dropped blocks in ARP	当 IP 地址解析为其相应的硬件地址时丢弃的块数。
Maximum queued blocks	在等待 IP 地址被解析时曾排入 ARP 模块队列的最大块数。
Queued blocks	当前排入 ARP 模块队列的块数。
Interface collision ARPs received	所有接口上收到的 IP 地址与接口 IP 地址相同的 ARP 数据包数量。
ARP-defense gratuitous ARPs sent	由设备作为 ARP 防御机制一部分发送的自然 ARP 数。
Total ARP retries	当地址在对第一个 ARP 请求的响应中未解析时由 ARP 模块发送的 ARP 请求总数。
Unresolved hosts	其 ARP 请求仍由 ARP 模块发出的未解析主机数。

字段	Description
Maximum unresolved hosts	自上次清除或设备启动后曾在 ARP 模块中的未解析主机最大数。

Related Commands

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp	显示 ARP 表。
show running-config all arp	显示 ARP 超时的当前配置。

show as-path-access-list

要显示所有当前自治系统 (AS) 路径访问列表的内容，请使用 **show as-path-access-list** 命令。

show as-path-access-list ［编号］

Syntax Description

number	（可选）指定 AS 路径访问列表序号。有效值介于 1 与 500 之间。

Command Default

如果没有指定 序号 参数，命令输出将显示所有 AS 路径访问列表。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show as-path-access-list** 命令的输出示例：

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

 AS path access list 2
```

show asp cluster counter

要调试群集技术环境中的全局或情景特定信息，请使用 **show asp cluster counter** 命令。

show asp cluster counter

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp cluster counter 命令显示全局和情景特定的 DP 计数器，可帮助您对问题进行故障排除。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp cluster counter** 命令的输出示例：

```
> 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

命令	Description
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp dispatch

要显示设备负载均衡 ASP 调度程序的统计信息（这对诊断性能问题非常有用），请使用 **show asp dispatch** 命令。它仅适用于混合轮询/中断模式的 threat defense virtual 设备。

show asp dispatch

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show asp dispatch** 命令的输出示例。

```
> 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

要调试加速安全路径丢弃的数据包或连接，请使用 **show asp drop** 命令。

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

Syntax Description

flow [*flow_drop_reason*]	（可选）显示丢弃的流量（连接）。您可以选择指定特定原因。使用 ?查看可能的流丢弃原因列表。
frame [*frame_drop_reason*]	（可选）显示丢弃的数据包。您可以选择指定特定原因。使用 ?查看可能的丢帧原因列表。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp drop 命令显示加速安全路径丢弃的数据包或连接，可帮助您对问题进行故障排除。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

有关可能的丢弃原因的信息，请参阅“显示 ASP 丢弃命令用法”文档，网址为 http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html。

示例

以下是 **show asp drop** 命令的输出示例，带有指示计数器上次清除时间的时间戳：

```
> 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

要调试数据路径或控制路径事件队列，请使用 **show asp event** 命令。

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

Syntax Description

dp-cp	显示从 ASP 数据路径发送到控制平面的事件。
cp-dp	显示从控制平面发送到 ASP 数据路径的事件。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp event 命令显示数据路径和控制路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp event dp-cp** 命令的输出示例：

```
> 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

要显示与绕过 Snort 检查的空 ACK 数据包相关的统计信息，请使用 **show asp inspect-dp ack-passthrough** 命令。

show asp inspect-dp ack-passthrough

Command History

版本	修改
7.0	引入了此命令。

使用指南

使用 **clear asp inspect-dp ack-passthrough** 命令重置这些统计信息。

示例

以下是输出示例。信息包括是否启用 ACK 传递，以及以下统计信息：

- 绕过的 ACK 数据包数 - 未转发到 Snort 进行检查的空 ACK 数据包的数量。
- 已发送的元 ACK - 发送到 Snort 的后续数据包上附带的空 ACK 的数量。此数字可能小于绕过的数据包数量，因为如果同一方向的后续数据包具有更高序列号的 ACK，则不需要且不包括先前保存的空 ACK 信息。

```
> 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

显示有关出口优化的统计信息，这是一项提高性能的功能。根据思科 TAC 的建议使用此命令。

show asp inspect-dp egress optimization

Command History

版本	修改
6.4	引入了此命令。

使用指南

show asp inspect-dp egress-optimization 命令显示有关符合出口优化条件的流的信息，出口优化是一种增强性能的功能。输出结果将显示以下信息：

- 当前运行状态：出口优化是启用还是禁用。
- 流（ 流 包含一个或多个 数据包）：
  - 当前：当前符合出口优化处理条件的流数量。
  - 最大值：自上次重新启动检测引擎或清除出口优化统计信息以来，符合出口优化条件的流量总数。
- 数据包：
  - 已处理：已处理的数据包总数。
  - 例外：最初被确定为符合出口优化条件，但后来被确定为不符合出口优化条件的数据包数量。

示例

以下是 **show asp inspect-dp egress-optimization** 命令的输出示例。

```
> 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

命令	Description
clear asp inspect-dp egress-optimization	清除出口优化统计信息。

命令	Description
show conn state egress_optimization	显示符合出口优化条件的流的相关信息。根据思科 TAC 的建议使用此命令。

show asp inspect-dp snort

要查看 PDTS（数据平面传输/接收队列到 Snort）环的快照，请使用 **show asp inspect-dp snapshot** 命令。

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

Syntax Description

config	显示 PDTS 快照的全局配置。
instance *instance_id*	显示指定 PDTS 使用者实例 ID 的快照。值范围为 0-2147483647。
queue *queue_id*	显示 PDTS 环的指定数据路径传输队列 ID 的快照。值范围为 0-2147483647。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp inspect-dp snapshot 命令显示 PDTS 环快照功能的全局配置。输出结果将显示以下信息：

- 最大快照数：允许的最大自动快照数。
- 当前正在使用：到目前为止已存储的快照数量。
- 间隔：时间间隔值指定允许在同一 PDTS 环上创建两个快照的时长
- 自动快照：显示是否启用或禁用自动 PDTS 快照功能

示例

以下是 **show asp inspect-dp snapshot config** 命令的输出示例。

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

以下是 **show asp inspect-dp snapshot instance** 命令的输出示例。

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

show asp inspect-dp snort

要显示所有 snort 实例的状态，请使用 **show asp inspect-dp snort** 命令。

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

Syntax Description

instance *instance_id*	显示特定 snort 实例的状态。的值范围为 0-2147483647。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示所有 snort 实例的状态。输出结果将显示以下信息：

- Id: Snort 实例 ID。
- PID：Snort 实例流程 ID。
- CPU 使用率：Snort 实例 ID 的 CPU 使用率。打印总数和用户/系统。**注意：** Firepower 2100 系列不显示此字段。
- 连接数：Snort 实例当前持有的连接数。
- 分段/数据包：Snort 实例当前处理的分段或数据包的数量。
- 状态：Snort 实例的状态。

示例

以下是 **show asp inspect-dp snort** 命令的输出示例。

```
> 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
```

以下是 Firepower 2100 上 **show asp inspect-dp snort** 命令的输出示例。

```
> 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

要显示 snort 实例的 PDTS 相关原始计数器，请使用 **show asp inspect-dp snort counters** 命令。

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

Syntax Description

instance *instance_id*	显示特定 snort 实例的计数器。值范围为 0-2147483647。
queues	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
rate	它需要 5 秒的计数器快照，平均为 1 秒，并显示计数器更改的速率。
debug	它会显示某些未以其他方式显示的调试计数器。
zeros	系统将显示所有计数器，包括零计数器。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 snort 实例的 PDTS 相关原始计数器。输出结果将显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- 类型：计数器的类型。数据计数器、错误计数器、调试计数器等。
- 名称：计数器的名称。
- 值：人类可读的计数器值。
- 原始值：计数器的原始值。

计数器名称：

- 发送字节数：Lina 发送到 snort 实例的字节数。
- 发送分段：Lina 发送到 snort 实例的帧/分段数。
- 接收字节数：Lina 从 snort 实例接收的字节数。
- 接收分段：Lina 从 snort 实例接收的帧/分段数。
- NewConns：发送到 snort 实例的连接数。
- RxQ-唤醒

- TxQ-唤醒
- TxQ-LB-Dynamic：启动 PDTS 动态负载均衡的次数。
- TxQ-Data-Hi-Thresh：达到 Lina 传输队列的高阈值限制的次数。
- RxQ-Full：Lina 的接收队列已满的次数。
- TxQ-Full：Lina 的传输队列已满的次数。
- TxQ-Data-Limit：达到 Lina 传输队列数据限制的次数。
- TxQ-LB-Failed：PDTS 动态负载均衡失败的次数。
- TxQ-Unavail：Lina 的传输队列不可用的次数。
- TxQ-Not-Ready：Lina 的传输队列未就绪的次数。
- TxQ-Suspended：Lina 的传输队列暂停的次数。
- RxQ-Unavail：Lina 的接收队列不可用的次数。
- RxQ-Not-Ready：Lina 的接收队列未就绪的次数。
- RxQ-Suspended：Lina 的接收队列暂停的次数。

示例

以下是 **show asp inspect-dp snort counters** 命令的输出示例。

```
> 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

要显示 snort 实例的 PDTS 相关计数器，请使用 **show asp inspect-dp snort counters summary** 命令。计数器汇总到每个实例。

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

Syntax Description

instance *instance_id*	显示特定 snort 实例的计数器。值范围为 0-2147483647。
queues	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
rate	显示计数器中的一秒平均增量。目前，一秒平均值基于命令的上次调用和当前调用之间的增量增量。这将更改，以便增量增加基于 5 秒滚动平均值，每秒采样一次。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 snort 实例的 PDTS 相关计数器。输出结果将显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- TxBytes：Lina 发送到 snort 实例的总字节数。
- TxFrames：Lina 发送到 snort 实例的帧/分段总数。
- RxBytes：Lina 从 snort 实例接收的总字节数。
- RxFrames：Lina 从 snort 实例接收的帧/网段总数。
- 连接：Snort 实例处理的连接总数。

示例

以下是 **show asp inspect-dp snort counters summary** 命令的输出示例。

```
> 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

要显示将所有队列汇聚到同一实例的所有 snort 实例（进程）的队列信息，请使用 **show asp inspect-dp snort queues** 命令。

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

Syntax Description

instance *instance_id*	显示特定 snort 实例的队列。值范围为 0-2147483647。
detail	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
debug	系统还会显示额外的调试信息。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示将所有队列汇聚到同一实例的所有 snort 实例（进程）的队列信息，输出显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- Rx 队列：Lina 的接收队列。“Used”表示数据量，“util”表示队列利用率，“state”表示共享内存状态。
- TxQ：Lina 的传输队列。“Used”表示数据量，“util”表示队列利用率，“state”表示共享内存状态。

Counters:

- RxQ-Size：Lina 的接收队列大小。
- TxQ-Size：Lina 的传输队列大小。
- TxQ-Data-Limit：传输队列的数据限制。一旦超过此阈值，数据包将被丢弃。百分比显示传输队列的阈值。
- TxQ-Data-Hi-Thresh：传输队列的高阈值。一旦超过此阈值，PDTS 动态负载均衡将开始尝试均衡流向其他 snort 实例的流量。

示例

以下是 **show asp inspect-dp snort queues** 命令的输出示例。

```
> 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

要显示 snort 队列耗尽时的自动快照，请使用 **show asp inspect-dp snort queue-exhaustion** 命令。

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

Syntax Description

snapshot *snapshot_id*	此选项指定用于打印队列耗尽信息的特定快照。值介于 1 和 24 之间。
export *location*	快照的内容将导出到指定位置的 pcap 文件中，以便进行机下分析。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp inspect-dp snort queue-exhaustion 命令显示 snort 队列耗尽时拍摄的快照的内容。它显示所选快照的内容。输出类似于 **show capture** 命令的输出。

示例

以下是 **show asp inspect-dp snort queue-exhaustion** 命令的输出示例。

```
> 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

要显示负载均衡器队列大小的直方图，请使用 **show asp load-balance** 命令。

show asp load-balance ［**detail**］

Syntax Description

detail	（可选）显示有关示例中使用的散列存储桶的详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp load-balance 命令可能会帮助您排除故障。通常，数据包将由从接口接收环拉入的同一核心进行处理。但是，如果另一个核心已经处理与刚接收的数据包相同的连接，则该数据包将排队至该核心。这种排队可能会导致负载均衡器队列增长，而其他核心处于空闲状态。有关详细信息，请参阅 **asp load-balance per-packet** 命令。

示例

以下是 **show asp load-balance** 命令的输出示例。X 轴表示在不同队列中排队的数据包数量。Y 轴表示有数据包排队的负载均衡器散列桶数量，请不要与直方图标题中的桶（指直方图桶）混淆。要了解拥有队列的散列桶的确切数量，请使用 **detail** 关键字。

```
> 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

命令	Description
asp load-balance per-packet	更改多核心 ASA 型号的核心负载平衡方法。

show asp multiprocessor accelerated- features

要调试加速安全路径多处理器加速，请使用 **show asp multiprocessor accelerated-features** 命令。

show asp multiprocessor accelerated-features

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp multiprocessor accelerated-features 命令显示为多处理器加速的功能列表，这可能有助于您解决性能问题。

示例

以下是 **show asp multiprocessor accelerated-features** 命令的输出示例：

```
> 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

要跟踪和显示自旋锁和异步丢失统计信息，请使用 **show asp overhead** 命令。

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

Syntax Description

sort-by-average	按每次调用的平均周期对结果进行排序
sort-by-file	按文件名对结果进行排序

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show asp overhead** 命令的输出示例：

```
> 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

要显示预过滤器策略快速路径的数据包数量、作为大型流进行了卸载、完全通过访问控制（Snort）进行评估，请使用 **show asp packet-profile** 命令。

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

Syntax Description

data-path	显示数据平面数据包配置文件的计数器。
offload	显示硬件负载分流数据包配置文件的计数器。
snort	显示 snort 数据包配置文件的计数器。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.5	引入了此命令。

使用指南

根据配置的访问策略、Snort 判定和数据流分流支持等硬件功能，通过 threat defense 设备的每个数据包都会经历不同的处理阶段。

全局计数器用于跟踪这些统计信息，并在每个会话结束时进行更新。这些全局计数器以直方图的形式收集和表示。在任何给定点，直方图都会显示自设备启动或上次重启以来系统处理的累积数据包计数器。

示例

以下是 **show asp packet-profile** 命令的输出示例。

```
> 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

要查看 tmatch 编译过程的状态，请使用 **show asp rule-engine** 命令。

show asp rule-engine

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示用作访问组的访问列表的编译正在进行还是已完成。编译时间取决于访问列表的大小。“开始”和“已完成”的时间状态对于所有规则都是通用的，因为它是一个批处理过程，而不是特定于模块。大多数模块元素计数将显示在表中。状态还显示 NAT 规则、路由、对象和接口编译。

```
> 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

要调试加速安全路径 ARP 表，请使用 **show asp table arp** 命令。

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

Syntax Description

address *ip_address*	（可选）标识您要查看 ARP 表条目的 IP 地址。
interface *interface_name*	（可选）标识您要查看 ARP 表的特定接口。
netmask *mask*	（可选）设置 IP 地址的子网掩码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show arp 命令显示控制层面的内容，而 **show asp table arp** 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table arp** 命令的输出示例：

```
> 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

命令	Description
show arp	显示 ARP 表。
show arp statistics	显示 ARP 统计信息。

show asp table classify

要调试加速安全路径分类器表，请使用 **show asp table classify** 命令。

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

Syntax Description

crypto	（可选）仅显示加密、解密和 ipsec 隧道流域。
domain *domain_name*	（可选）显示特定分类器域的条目。有关可用域的列表，请参阅 CLI 帮助。
hits	（可选）显示具有非零命中值的分类器条目。
interface *interface_name*	（可选）标识您要查看分类器表的特定接口。
match *regexp*	（可选）显示匹配正则表达式的分类器条目。正则表达式包含空格时请使用引号。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table classify 命令显示加速安全路径的分类器内容，可帮助您对问题进行故障排除。分类器检查传入数据包的属性（例如协议）以及源和目的地址，从而将每个数据包匹配适当的分类规则。每个规则均使用确定执行何种类型操作（例如丢弃数据包还是允许其通过）的分类域进行标记。所示信息仅用于调试目的，输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table classify** 命令的输出示例：

```
> 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
```

```
...
```

以下是 **show asp table classify hits** 命令的输出示例，带有上次清除命中计数器的记录：

```
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
```

以下是来自包含 Layer 2 信息地 **show asp table classify hits** 命令的输出示例：

```
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

要调试用于群集技术的加速安全路径 cHash 表，请使用 **show asp table cluster chash-table** 命令。

show asp table cluster chash-table

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table cluster chash-table 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table cluster chash-table** 命令的输出示例：

```
> 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

命令	Description
show asp cluster counter	显示集群数据路径计数器信息。

show asp table interfaces

要调试加速安全路径接口表，请使用 **show asp table interfaces** 命令。

show asp table interfaces

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table interfaces 命令显示加速安全路径的接口表内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table interfaces** 命令的输出示例：

```
> 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

要调试加速安全路径网络服务对象表，请使用 **show asp table network-service** 命令。

show asp table network-service

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示如何显示网络服务对象表：

```
> 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

要调试加速安全路径路由表，请使用 **show asp table routing** 命令。此命令支持 IPv4 和 IPv6 地址。

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

Syntax Description

address *ip_address*	设置您要查看路由条目的IP地址。对于IPv6地址，您可以包含子网掩码，形式为斜线 (/) 后跟前缀（0 至 128）。例如，输入 fe80::2e0:b6ff:fe01:3b7a/128。
input	显示输入路由表的条目。
interface *interface_name*	（可选）标识您要查看路由表的特定接口。
netmask *mask*	对于 IPv4 地址，指定子网掩码。
output	显示输出路由表的条目。
management-only	显示管理路由表中的号码携带路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show asp table routing 命令显示加速安全路径的路由表内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科TAC以帮助您使用此命令调试您的系统。management-only 关键字显示管理路由表中的号码可携带性路由。

示例

以下是 **show asp table routing** 命令的输出示例：

```
> 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
```

以下示例显示名为 alpha 的虚拟路由器的路由表。

```
> 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

命令	Description
show route	在控制层面中显示路由表。

show asp table socket

要帮助调试加速安全路径套接字信息，请使用 **show asp table socket** 命令。

show asp table socket ［处理］［**stats**］

Syntax Description

处理	指定套接字的长度。
stats	显示加速安全路径套接字表的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table socket 命令显示加速安全路径套接字信息，可在对加速安全路径套接字问题进行故障排除时提供帮助。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table socket** 命令的输出示例。

```
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
```

以下是 **show asp table socket stats** 命令的输出示例。

```
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统计信息是数据包计数器，表示指向设备上运行或侦听的服务（例如Telnet、SSH或HTTPS）的发送或接收数据包数量。校验和错误是由于计算的数据包校验和不匹配数据包中存储的校验和值（也就是说，数据包已损坏）而丢弃的数据包数量。NP SSL统计信息指示收到的每种类型的消息数量。大多数消息均指示开始和结束到SSL服务器或SSL客户端实例的新SSL连接。

Related Commands

命令	Description
show asp table vpn-context	显示加速安全路径VPN情景表。

show asp table vpn-context

要调试加速安全路径 VPN 情景表，请使用 **show asp table vpn-context** 命令。

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

Syntax Description

detail	（可选）显示 VPN 情景表的更多详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table vpn-context 命令显示加速安全路径的 VPN 情景内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table vpn-context** 命令的输出示例：

```
> 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
...
```

以下是启用永久 IPsec 隧道流功能后（如 PRESERVE 标记所示） **show asp table vpn-context** 命令的输出示例：

```
> 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
```

以下是 **show asp table vpn-context detail** 命令的输出示例。启用持久 IPsec 隧道流量功能后，这些标志将包括 PRESERVE 标志。

```
> 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

命令	Description
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp table zone

要调试加速安全路径区域表，请使用 **show asp table zone** 命令。

show asp table zone

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table zone 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table zone** 命令的输出示例。在本示例中，名为 is-154 的区域实际上是一个内联集，而不是流量区域。

```
> 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

命令	Description
show inline-set	显示内联集。
show zone	显示流量区域。

show audit-log

要显示系统审核日志，请使用 **show audit-log** 命令。

show audit-log

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令按时间倒序显示审核日志；首先列出最近的审核日志事件。

事件可能包括系统更新、权限问题、配置更改和策略应用。此信息仅适用于管理中心远程管理的设备。本地托管系统的审核日志为空。

示例

以下示例显示了审核日志。

```
> 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
-------------------------------------------------------------
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。