show s - sz

- show sctp， 第 3 页
- show serial-number， 第 5 页
- show service-policy， 第 6 页
- show shun， 第 12 页
- show sip， 第 13 页
- show skinny， 第 14 页
- show sla monitor， 第 15 页
- show snmp-server， 第 17 页
- show snort counters， 第 20 页
- show snort instances， 第 23 页
- show snort preprocessor-memory-usage， 第 24 页
- show snort statistics， 第 26 页
- show snort tls-offload， 第 29 页
- show software authenticity， 第 31 页
- show ssd， 第 34 页
- show ssh-access-list， 第 35 页
- show ssl， 第 36 页
- show ssl-policy-config， 第 39 页
- show ssl-protocol， 第 41 页
- show startup-config， 第 42 页
- show summary， 第 43 页
- show sunrpc-server active， 第 44 页
- show switch mac-address-table， 第 45 页
- show switch vlan， 第 47 页
- show tcpstat， 第 49 页
- show tech-support， 第 52 页
- show threat-detection memory， 第 53 页
- show threat-detection rate， 第 55 页
- show threat-detection scanning-threat， 第 57 页
- show threat-detection shun， 第 58 页

- show threat-detection statistics， 第 59 页
- show time， 第 68 页
- show time-range， 第 69 页
- show tls-proxy， 第 70 页
- show track， 第 72 页
- show traffic， 第 73 页
- show upgrade， 第 74 页
- show user， 第 76 页
- show version， 第 78 页
- show vlan， 第 80 页
- show vm， 第 81 页
- show vpdn， 第 82 页
- show vpn load-balancing， 第 84 页
- show vpn-sessiondb， 第 85 页
- show vpn-sessiondb ratio， 第 97 页
- show vpn-sessiondb summary， 第 99 页
- show vrf，第 101 页
- show wccp，第 103 页
- show webvpn，第 105 页
- show xlate，第 108 页
- show zone，第 110 页
- shun，第 112 页
- shutdown，第 114 页
- system access-control clear-rule-counts，第 115 页
- system generate-troubleshoot，第 116 页
- system lockdown-sensor，第 118 页
- system support commands，第 119 页
- system support ssl-client-hello- commands，第 120 页
- system support diagnostic-cli，第 121 页
- system support ssl-hw- commands，第 123 页
- system support view-files，第 126 页

show sctp

要显示当前的流控制传输协议 (SCTP) Cookie 和关联，请使用 **show sctp** 命令。

show sctp ［**detail**］

Syntax Description

detail	显示 SCTP 关联的详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

命令显示有关 SCTP Cookie 和关联的信息。**show sctp**

如果使用 管理中心FlexConfig 启用 SCTP 检测，则此命令可以显示 SCTP 信息。

示例

以下是 **show sctp** 命令的输出示例：

```
> show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

以下是 **show sctp detail** 命令的输出示例：

```
> show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

Related Commands

命令	Description
show local-host	显示主机上有关使连接在每个接口上通过设备的信息。
show service-policy inspect sctp	显示 SCTP 检测统计信息。
show traffic	显示每个接口的连接和检测统计信息

show serial-number

要显示印刷电路板 (PCB) 序列号，请使用 **show serial-number** 命令。此命令不适用于虚拟设备。

show serial-number

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show serial-number** 命令查看印刷电路板的序列号。此信息也显示在 **show version system** 和 **show running-config** 输出中。

使用 **show inventory** 命令查看机箱序列号

示例

以下示例显示如何显示序列号。此示例中的数字已更改为无效。

```
> show serial-number
XXX175078X5
```

show service-policy

要显示服务策略统计信息，请使用 **show service-policy** 命令。

show service-policy [**global** | **interface** *intf*] [**cluster flow-mobility** | **inspect** *inspection* [*arguments*] | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]
show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

cluster flow-mobility	（可选。）显示有关 threat defense 集群中流移动性的状态信息。
dest_ip dest_mask	对应 **flow** 关键字，指流量流的目标 IP 地址和子网掩码。
details	（可选）对应 **set connection** 关键字，如果启用每客户端连接限制，则显示每客户端连接信息。
eq *dest_port*	（可选）对应 **flow** 关键字，等于流的目标端口。
eq *src_port*	（可选）对应 **flow** 关键字，等于流的源端口。
flow 协议	（可选）显示与通过 5 元组（协议、源 IP 地址、源端口、目标 IP 地址、目标端口）标识的特定流匹配的策略。您可以使用此命令检查服务策略配置是否将提供特定连接所需的服务。
global	（可选）限制全局策略的输出。
host *dest_host*	对应 **flow** 关键字，指流量流的主机目标 IP 地址。
host *src_host*	对应 **flow** 关键字，指流量流的主机源 IP 地址。
icmp_control_message	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 控制消息。
icmp_number	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 协议编号。
inspect *inspection* [*arguments*]	（可选）显示有关包括 **inspect** 命令的策略的详细信息。并非所有 **inspect** 命令都受到详细输出支持。要查看所有检测，请使用 **show service-policy inspect ?** 命令。各个检查的可用参数各不相同；请参阅 CLI 帮助以获取更多信息。
interface *intf*	（可选）显示应用到通过 *intf* 参数指定的接口的策略，其中 *intf* 是接口名称。
police	（可选）显示有关包括 **police** 命令的策略的详细信息。
priority	（可选）显示有关包括 **priority** 命令的策略的详细信息。

set connection	（可选）显示有关包括 **set connection** 命令的策略的详细信息。
sfr	（可选）显示有关 ASA FirePOWER 模块策略的详细信息。此关键字对 threat defense无意义。
shape	（可选）显示有关包括 **shape** 命令的策略的详细信息。
src_ip src_mask	对应 **flow** 关键字，指流量流中使用的源 IP 地址和子网掩码。
user-statistics	（可选）显示有关包括 **user-statistics** 命令的策略的详细信息。此关键字对 threat defense无意义。

Command Default

如果不指定任何参数，此命令将显示所有全局接口策略。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show service-policy 命令输出中显示的初期连接数表示与为流量类定义的流量匹配的接口的当前初期连接数。“embryonic-conn-max”字段显示为流量类配置的最大初期限制。如果所显示的当前初期连接数等于或超过最大值，将对与流量类型相匹配的新 TCP 连接应用 TCP 拦截。

当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。**show** 命令输出不会包含有关旧连接的数据。要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略重新连接。请参阅 **clear conn** 或 **clear local-host** 命令。

不能直接使用 管理中心 或 设备管理器配置服务策略。编辑各种连接设置或配置 QoS 策略时，会间接进行一些更改。您还可以使用 **configure inspection** 命令调整启用的默认检测。如果在 管理中心 中使用 FlexConfig 配置服务策略，则此命令显示与配置相关的统计信息 。

注释 对于 **inspect icmp** 和 **inspect icmp error** 策略，数据包计数仅包括回应请求和应答数据包。

示例

以下是 **show service-policy** 命令的输出示例。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
```

```
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

对于具有多个 CPU 核心的设备，有一个锁定失败计数器。锁定机制用于保护共享数据结构和变量，因为它们可以被多个核心使用。当核心获取锁失败时，它会尝试再次获取锁。每次尝试失败时，锁定失败计数器都会递增。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

以下命令显示 GTP 检查的统计信息。示例后面的表中对输出进行了说明。

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
```

```
unknown_msg                     0     unexpected_sig_msg        0
unexpected_data_msg             0     ie_duplicated             0
mandatory_ie_missing            0     mandatory_ie_incorrect    0
optional_ie_incorrect           0     ie_unknown                0
ie_out_of_order                 0     ie_unexpected             0
total_forwarded                67     total_dropped             1
signalling_msg_dropped          1     data_msg_dropped          0
signalling_msg_forwarded       67     data_msg_forwarded        0
total created_pdp              33     total deleted_pdp        32
total created_pdpmcb           31     total deleted_pdpmcb     30
total dup_sig_mcbinfo           0     total dup_data_mcbinfo    0
no_new_sgw_sig_mcbinfo          0     no_new_sgw_data_mcbinfo   0
pdp_non_existent                1
```

表 *1: GPRS GTP Statistics*

列标题	Description
version_not_support	显示具有不支持的 GTP 版本字段的数据包。
msg_too_short	显示长度小于 8 字节的数据包。
unknown_msg	显示未知类型消息。
unexpected_sig_msg	显示意外的信令消息。
unexpected_data_msg	显示意外数据消息。
mandatory_ie_missing	显示缺少必需信息元素 (IE) 的消息。
mandatory_ie_incorrect	显示具有格式不正确的必需信息元素 (IE) 的消息。
optional_ie_incorrect	显示可选信息元素 (IE) 无效的消息。
ie_unknown	显示具有未知信息元素 (IE) 的消息。
ie_out_of_order	显示具有失序信息元素 (IE) 的消息。
ie_unexpected	显示具有意外信息元素 (IE) 的消息。
ie_duplicated	显示具有重复信息元素 (IE) 的邮件。
optional_ie_incorrect	显示具有格式不正确的可选信息元素 (IE) 的消息。
total_dropped	显示丢弃的消息总数。
signalling_msg_dropped	显示丢弃的信令消息数。
data_msg_dropped	显示丢弃的数据消息数。
total_forwarded	显示转发的消息总数。
signalling_msg_forwarded	显示转发的信令消息数。

列标题	Description
data_msg_forwarded	显示转发的数据消息数。
total created_pdp	显示所创建的数据包数据协议 (PDP) 承载情景总数。
total deleted_pdp	显示所创建的数据包数据协议 (PDP) 承载情景总数。
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	这些字段与 PDP 主控制块的使用相关，这是一项实施功能。这些计数器由思科技术支持人员用于故障排除，最终用户并不直接感兴趣。
pdp_non_existent	显示为不存在的 PDP 情景接收的消息数。

以下命令显示有关 PDP 情景的信息：

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,       Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,       Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,       Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

下表介绍了 **show service-policy inspect gtp pdp-context** 命令的输出。

表 *2: PDP* 情景

列标题	Description
Version	显示 GTP 版本。
TID	显示隧道标识符。
MS Addr	显示移动站地址。
SGSN Addr SGW Addr	显示服务网关服务节点 (SGSN) 或服务网关 (SGW)。
Idle	显示未使用 PDP 或承载情景的时间。
APN	显示接入点名称。

Related Commands

命令	Description
clear service-policy	清除所有服务策略统计信息。
configure inspection	启用或禁用默认检测。
show running-config service-policy	显示在运行配置中配置的服务策略。

show shun

要显示避开信息，请使用 **show shun** 命令。

show shun ［*src_ip* | **statistics**］

Syntax Description

src_ip	（可选）显示该地址的信息。
statistics	（可选）显示接口规避统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show shun** 命令的输出示例：

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

命令	Description
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
shun	阻止新连接并禁止通过任何现有连接传输数据包，从而允许对攻击主机作出动态响应。

show sip

要显示 SIP 会话，请使用 **show sip** 命令。

show sip

Command History

版本	修改
6.1	引入了此命令。

使用指南

show sip 命令显示有关通过 threat defense 设备建立的 SIP 会话的信息。

示例

以下是 **show sip** 命令的输出示例：

```
> show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

此示例显示 threat defense 设备中的两个活动 SIP 会话（如 Total 字段中所示）。每个呼叫 ID 代表一个呼叫。

第一个会话（其呼叫 ID 为 c3943000-960ca-2e43-228f@10.130.56.44）处于 Call Init 状态，这意味着会话仍处于呼叫建立阶段。只有看到 ACK 时，才说明呼叫设置完成。此会话已空闲 1 秒。

第二个会话处于 Active 状态，这表示呼叫建立已完成，且终端正在交换媒体。此会话已空闲 6 秒。

Related Commands

命令	Description
show conn	显示不同连接类型的连接状态。

show skinny

要显示 SCCP（瘦客户端）会话的信息，请使用 **show skinny** 命令。

show skinny ［**audio** | **video**］

Syntax Description

audio	显示 SCCP 音频会话
video	显示 SCCP 视频会话

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show skinny** 命令在以下情况时的输出示例。设备中设置了两个活动瘦客户端会话。第一个建立在位于本地地址 10.0.0.11 的内部思科 IP 电话与位于 172.18.1.33 的外部思科统一通信管理器之间。TCP 端口 2000 是思科统一通信管理器。第二个建立在位于本地地址 10.0.0.22 的另一个内部思科 IP 电话与同一思科统一通信管理器之间。

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                    FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

输出表明已在两个内部思科 IP 电话之间建立呼叫。第一个电话和第二个电话的 RTP 侦听端口分别为 UDP 22948 和 20798。

Related Commands

命令	Description
show conn	显示不同连接类型的连接状态。

show sla monitor

要显示有关互联网协议服务水平协议 (IP SLA) 的信息，请使用 **show sla monitor** 命令。

show sla monitor {**configuration** | **operational-state**} [*sla_id*]

Syntax Description

configuration	显示 SLA 配置值，包括默认值。
operational-state	显示 SLA 操作的运行状态。
sla_id	（可选）SLA 操作的 ID 编号。有效值范围为 1 至 2147483647。

Command Default

如果未指定 SLA ID，将显示所有 SLA 操作的配置值。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show running-config sla monitor** 命令查看运行配置中的 SLA 操作命令。

示例

以下是 **show sla monitor configuration** 命令的输出示例。它显示 SLA 操作 124 的配置值。**show sla monitor configuration** 命令输出之后是相同 SLA 操作的 **show running-config sla monitor** 命令输出。

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

> show running-config sla monitor 124

sla monitor 124
```

```
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

以下是 **show sla monitor operational-state** 命令的输出示例：

```
> show sla monitor operational-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Related Commands

命令	Description
show running-config sla monitor	显示运行配置中的 SLA 操作配置命令。

show snmp-server

要显示有关设备上配置的 SNMP 服务器的信息，请使用 **show snmp-server** 命令。

show snmp-server {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

Syntax Description

engineID	显示 SNMP 引擎的标识。
group	显示已配置的SNMP组的名称、正在使用的安全模型、不同视图的状态以及每个组的存储类型。
host	显示属于主机组的已配置SNMP主机的名称、正在使用的接口以及正在使用的 SNMP 版本。
statistics	显示 SNMP 服务器统计信息。
user [*username*]	显示有关SNMP用户的特征的信息。您可以选择指定用户名，以将信息限制为该用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

SNMP 引擎是可以驻留在本地设备上的 SNMP 副本。引擎 ID 是为每个 SNMP 代理分配的唯一值。引擎 ID 不能配置。引擎 ID 的长度为 25 字节，用于生成加密密码。在故障转移对中，引擎 ID 与对等设备同步。

根据 SNMP 的基于视图的访问控制模型 (VACM) 来使用 SNMP 用户和组。SNMP 组确定要使用的安全模型。SNMP 用户应当符合 SNMP 组的安全模型。每个 SNMP 组名称/安全级别对必须唯一。

注释 统计信息显示有关 SNMP 模块的输入和输出数据包的信息。数据包被输出并不意味着它们到达目的地。路由问题、干预防火墙、拔出接口等可能会阻止输出数据包的传输。如果数据包未到达 SNMP 服务器，请使用 **show asp drop** 和 **show logging** 等命令检查其他问题。

示例

以下是 **show snmp-server engineid** 命令的输出示例：

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

以下是 **show snmp-server group** 命令的输出示例：

```
> show snmp-server group
```

```
groupname: public                           security model:v1
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                           security model:v2c
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                    security model:v3 priv
readview : def_read_view                writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

以下是 **show snmp-server host** 命令的输出示例，其中仅显示轮询设备的活动主机：

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

以下是 **show snmp-server user** 命令的输出示例：

```
> show snmp-server user authuser
User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

输出提供以下信息：

- 用户名，是标识 SNMP 用户名称的字符串。
- 引擎 ID，是标识设备上的 SNMP 副本的字符串。
- 存储类型，指示在设备上的易失性或临时内存中还是在非易失性或永久内存中设定设置，如果为后者，则关闭设备再重新开启后，设置仍然保留。
- 活动访问列表，是与 SNMP 用户关联的标准 IP 访问列表。
- Rowstatus，指示其是否处于活动状态。
- 身份验证协议，标识正在使用哪种身份验证协议。选项为 MD5、SHA 或无。如果您的软件映像不支持身份验证，则此字段不显示。
- 隐私协议，指示是否启用 DES 数据包加密。如果您的软件映像不支持隐私，则此字段不显示。
- 组名称，指示用户所属的 SNMP 组。SNMP 组按照基于视图的访问控制模型 (VACM) 进行定义。

Related Commands

命令	Description
clear snmp-server statistics	清除 SNMP 数据包输入和输出计数器。
show running-config snmp-server	显示 SNMP 服务器配置。

show snort counters

要显示 Snort 预处理器连接的统计信息，请使用 **show snort counters** 命令。

show snort counters {**action** | **stream** | **sip** | **ssl** | **smtp** | **vrf**} {**all** | **instance** *x*}

Syntax Description

action	显示操作、限制和判定的 Snort 实例级统计信息。
stream	显示数据流预处理器的统计信息。
sip	显示 SIP 预处理器的统计信息。
ssl	显示 SSL 预处理器的统计信息。
smtp	显示 SMTP 预处理器的统计信息。
vrf	显示通过每个虚拟路由器的实时会话数。
all	显示系统中所有 Snort 实例的统计信息。例如，**show snort counters action all**、 **show snort counters smtp all**等。
instance *x*	显示系统中所选 Snort 实例的统计信息。例如，**show snort counters smtp instance 11**。使用 **show snort instances** 命令确定可用的实例编号。

Command History

版本	修改
6.3	引入了此命令。
6.6	添加了 **vrf** 关键字。

使用指南

使用此命令可显示系统中 Snort 实例的统计信息。您可以将这些统计信息用于提供信息和调试目的。请咨询思科 TAC 以帮助您使用此命令调试您的系统。使用 **show snort counters action all** 命令查看系统中所有 Snort 实例的操作、限制和判定的 Snort 实例级统计信息。使用 **show snort instances** 命令确定可用的实例编号。

以下示例显示系统中所有 Snort 实例的操作、限制和判定的 Snort 实例级统计信息。

```
> show snort counters action all
Instance : 1
------------

Action Stats are not available
 Total Action Processed:           0

...

================================================================================

Instance : 16
```

```
------------

Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       220009 (100.000%)
      Block:         5076 (  2.307%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)

================================================================================
```

以下示例显示了 Steam 统计信息。

```
> show snort counters stream all
Instance : 1
------------

Stream statistics not available
 Total sessions: 0
================================================================================

...

Instance : 16
------------

Stream statistics:
            Total sessions: 665
              TCP sessions: 665
              UDP sessions: 0
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 0
TCP StreamTrackers Deleted: 0
              TCP Timeouts: 661
              TCP Overlaps: 0
       TCP Segments Queued: 0
     TCP Segments Released: 0
       TCP Rebuilt Packets: 0
         TCP Segments Used: 0
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 0
      UDP Sessions Deleted: 0
```

```
               UDP Timeouts: 0
               UDP Discards: 0
                     Events: 0
            Internal Events: 0
            TCP Port Filter
                   Filtered: 0
                  Inspected: 0
                    Tracked: 910736
            UDP Port Filter
                   Filtered: 0
                  Inspected: 0
                    Tracked: 0

===============================================================================
```

以下示例显示了 Snort 实例 1 的 SMTP 统计信息。

```
> show snort counters smtp instance 1
Instance : 1
------------

SMTP Preprocessor Statistics
  Total sessions                                  : 80
  Max concurrent sessions                         : 1
  Base64 attachments decoded                      : 0
  Total Base64 decoded bytes                      : 0
  Quoted-Printable attachments decoded            : 0
  Total Quoted decoded bytes                      : 0
  UU attachments decoded                          : 0
  Total UU decoded bytes                          : 0
  Non-Encoded MIME attachments extracted          : 0
  Total Non-Encoded MIME bytes extracted          : 0

===============================================================================
```

Related Commands

命令	Description
clear snort statistics	清除 Snort 检测统计信息。
show snort statistics	显示 Snort 检查流量时与各种 Snort 判定匹配的数据包数。
show snort tls-offload	显示与硬件中的检测引擎 (Snort) 加密和解密的数据包相关的统计信息。

show snort instances

要显示可在其他 **show snort** 命令中使用的 Snort 实例编号列表，请使用 **show snort instances** 命令。

show snort instances

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 Snort 实例列表。

```
> show snort instances
Total number of instances available - 2

+----------+---------+
| INSTANCE |   PID   |
+----------+---------+
|    1     |   2787  |
|    2     |   2788  |
+----------+---------+
```

show snort preprocessor-memory-usage

要显示每个 Snort 实例的 Snort 预处理器的内存使用情况统计信息，请使用 **show snort preprocessor-memory-usage** 命令。

show snort preprocessor-memory-usage 实例*_ID* {**all** | **imap** | **pop** | **smtp**}

Syntax Description

实例*_ID*	Snort 实例的 ID 编号。使用 **show snort instances** 命令获取系统上活动的实例 ID 编号的列表。
all	显示所有预处理器的统计信息。
imap	仅显示 IMAP 预处理器的统计信息。
pop	仅显示 POP 预处理器的统计信息。
smtp	仅显示 SMTP 预处理器的统计信息。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 Snort 实例 1 的 SMTP 预处理器的统计信息。系统将提示您输入管理员密码。

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
---------------------------------


Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
       Total Sessions seen: 0
   Max concurrent sessions: 0
   Current Active sessions: 0

   Memory Pool:
        Free Memory:
            SMTP Mime Pool:       17968000 bytes
                 SMTP Pool:              0 bytes
```

```
        Used Memory:
            SMTP Mime Pool:              0 bytes
                 SMTP Pool:              0 bytes
        -------------------       ---------------
        Total Memory:             17968000 bytes

   Heap Memory:
                      Session:              0 bytes
                Configuration:          16784 bytes
                --------------         ------------
                 Total Memory:          16784 bytes
                 No of allocs:             38 times
                  IP sessions:             30 times
-----------------------------------------------------
```

show snort statistics

要在 Snort 检查流量时显示与各种 Snort 判定匹配的数据包数，请使用 **show snort statistics** 命令。

show snort statistics

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

使用此命令可显示访问策略和入侵规则配置的 Snort 检查结果。此命令通常用于调试意外的 Snort 检查行为。统计信息包括以下内容：

- 通过的数据包数 - 从 Lina 发送到 Snort 的数据包数。
- 阻止的数据包数 - 在 Lina 中阻止且未发送到 Snort 的数据包数量。
- 注入的数据包-Snort 创建并添加到流量流的数据包数。例如，如果配置具有重置操作的阻止，Snort 会生成数据包以重置连接。
- 绕过的数据包数（Snort 关闭或 Snort 繁忙）- 如果将系统配置为允许需要 Snort 检测的数据包，而 Snort 无法执行检测，则这些计数器是当 Snort 关闭或太忙而无法处理检测时绕过检测的数据包的数量数据包。

⚠

注意 当流被绕过（未经检查而通过）时，这些繁忙和关闭计数器会增加，直到被绕过的会话结束，即使 Snort 不再繁忙或关闭，也会发生这种情况。例如，如果持续数天的 TCP 连接在 Snort 繁忙或关闭时发送数据包，然后在 Snort 恢复后继续连接，则计数器可能会增加数天。

- 快速转发流-由策略快速转发并因此未检查的流的数量。
- 黑名单流-Snort 在策略配置中丢弃的流数。
- 流开始事件-当数据平面流程快速传输流而不将其发送到 Snort 时，Lina 进程会向 Snort 发送流开始事件。这些事件有助于 Snort 跟踪连接并报告连接事件。
- 流结束事件-当快速路径流结束时，Lina 流程会向 Snort 发送流结束事件。
- 拒绝流事件-当数据平面决定在将流发送到 Snort 之前丢弃流时，Lina 流程会向 Snort 发送拒绝流事件。
- 丢弃前转发到 Snort 的帧数 - 仅适用于 NGIPS 接口。这是转发到 Snort 的待丢弃数据包数。当 Lina 流程因某种原因（TCP 信头长度无效、UDP 长度无效或 IP 长度无效）而决定丢弃帧时，这些帧也会发送到 Snort 进行查看。
- 丢弃的注入数据包-Snort 添加到已丢弃的流量流的数据包数。

示例

以下示例脚本显示了 **show snort statistics** 命令显示的信息：

```
show snort statistics
Packet Counters:
  Passed Packets                                         6
  Blocked Packets                                        321
  Injected Packets                                       284
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

在下面的示例中，请考虑将访问控制策略配置为阻止并重置所有流量的情况。Lina无法处理重置，因此它将数据包升级到 Snort 以阻止并将重置注入客户端和服务器。

- 通过的数据包 - 显示从 Lina 传递到 Snort 的八个数据包。
- 注入的数据包 - 显示发送到客户端和服务器的两个数据包。
- 列入黑名单的流 - 显示 Snort 要求 Lina 阻止的流。

注释 本例中没有 被阻止的 数据包。

```
> show snort statistics
Packet Counters:
  Passed Packets                                         8
  Blocked Packets                                        0
  Injected Packets                                       2
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      3

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

在下面的示例中，请考虑以下情况：访问控制策略有一个规则与 FTP 端口匹配并具有阻止操作，另一个规则与 HTTP 应用匹配并具有允许操作。

- 通过的数据包 - 显示 60 个 HTTP 数据包，因为 Lina 将允许规则的数据包发送到 Snort。
- 拒绝流事件 - 显示 Lina 使用 FTP 端口匹配处理的两个数据和控制信道数据包。

注释 本例中没有 被阻止的 数据包。

```
> show snort statistics
Packet Counters:
  Passed Packets                                    60
  Blocked Packets                                   0
  Injected Packets                                  0
  Packets bypassed (Snort Down)                     0
  Packets bypassed (Snort Busy)                     0

Flow Counters:
  Fast-Forwarded Flows                              0
  Blacklisted Flows                                 0

Miscellaneous Counters:
  Start-of-Flow events                              0
  End-of-Flow events                                0
  Denied flow events                                2
  Frames forwarded to Snort before drop             0
  Inject packets dropped                            0
```

Related Commands

命令	Description
clear snort statistics	清除 Snort 检测统计信息。
configure snort preserve-connection	决定是否在 Snort 流程关闭时保留路由和透明接口上的现有 TCP/UDP 连接。

show snort tls-offload

要在硬件中显示与检测引擎 (Snort) 加密和解密的数据包相关的统计信息，请使用 **show snort tls-offload** 命令。此命令仅在以下支持 SSL 硬件加速的受管设备上可用：

- 采用 威胁防御 的 Firepower 2100
- 采用 威胁防御的 Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。

show snort tls-offload [proxy | tracker | description]

Syntax Description

proxy	（可选。）仅显示代理的统计信息。
tracker	（可选。）仅显示跟踪器的统计信息。
description	（可选。）显示代理和跟踪器的计数器说明。

Command History

版本	修改
6.2.3	引入了此命令。

使用指南

使用此命令可显示Snort的代理和跟踪器组件的详细统计信息。您可以将这些统计信息用于提供信息和调试目的。使用 **show snort tls-offload description** 命令查看计数器的说明。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

以下是 **show snort tls-offload** 命令示例：

```
====== Tracker Statistics ======
TOTAL_CONNECTION                 2774
TOTAL_RSA_KEY_EXCHANGE_4K        2774
TOTAL_CIPHER_SUITE_ENCR_AES      2774
TOTAL_CIPHER_SUITE_HASH_SHA1     2774
TOTAL_CKE_PMS_DECRYPTED          2774
TOTAL_RECORD_DECRYPTED           363001
TOTAL_RECORD_ENCRYPTED           363001
TOTAL_CONNECTION_W_DUR (<0.5s)   2771
AVG_CONNECTION_DURATION  (ms)    184
AVG_HANDSHAKE_TIME       (ms)    37
AVG_CKE_PMS_DECRYPT_TIME (us)    21402
AVG_RECORD_DECRYPT_TIME  (us)    619
AVG_RECORD_ENCRYPT_TIME  (us)    477
PEAK_CONNECTION_DURATION (ms)    400
PEAK_HANDSHAKE_TIME      (ms)    62
CONCURRENT_CONNECTION/Peak       3/3
CPS_ATTEMPTED/Peak               7/8
CPS_COMPLETED/Peak               8/8
```

```
CKE_PMS_DECRYPTING_Q/Peak         0/2
SKE_DH_PARAM_SIGNING_Q/Peak       0/0
RECORD_ENCRYPTING_Q/Peak          1/25
RECORD_DECRYPTING_Q/Peak          1/2
======= Proxy Statistics =======
TOTAL_CONNECTION(LW+FP)           15855
TOTAL_CONNECTION_FP               15853
CONNECTION_FP_RECV_FIN            31697
CONNECTION_FP_RECV_RST            27
CONNECTION_LW_RECV_FIN            2
CONCURRENT_CONNECTION_LW/Peak     0/2
CONCURRENT_CONNECTION_FP/Peak     3/7
BYPASS_NOT_ENOUGH_MEM             0
```

Related Commands

命令	Description
clear snort tls-offload	清除统计信息计数器。
debug snort tls-offload	显示所有 Snort 流程的所有类型的错误调试消息。

show software authenticity

要显示软件真实性信息，请使用 **show software authenticity** 命令。

show software authenticity {**development** | **file** *filename* | **keys** | **running**}

Syntax Description

development	显示是否已启用或禁用开发密钥签名映像的加载。
file *filename*	显示与特定映像文件的软件身份验证有关的数字签名信息。
keys	显示有关存储在 SPI 闪存中的开发密钥和释放密钥的信息。
running	显示与当前运行的映像文件的软件身份验证相关的数字签名信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

文件和运行映像的输出提供以下信息。

- 文件名，是内存中文件的名称。
- 映像类型，是所显示映像的类型。
- 签名者信息指定签名信息，其中包括以下内容：
  - 公用名称，是软件制造商的名称。
  - 组织单位，指示部署软件映像的硬件。
  - 组织名称，是软件映像的所有者。
- 证书序列号，是数字签名的证书序列号。
- 散列算法，指示数字签名验证中使用的散列算法类型。
- 签名算法，标识数字签名验证中使用的签名算法类型。
- 密钥版本，指示用于验证的密钥版本。

示例

以下是 **show software authenticity development** 命令的输出示例：

```
> show software authenticity development
Loading of development images is disabled
```

以下是 **show software authenticity file** 命令的输出示例。在本例中，文件是开发映像。对于当前在设备上运行的映像文件，您会看到相同的 **show software authenticity running** 输出。

```
> show software authenticity file os.img
File Name                       : disk0:/os.img
Image type                      : Development
    Signer Information
        Common Name             : abraxas
        Organization Unit       : NCS_Kenton_ASA
        Organization Name       : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm              : SHA2 512
    Signature Algorithm         : 2048-bit RSA
    Key Version                 : A
```

以下是 show software authenticity keys 命令的输出示例：

```
> show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
```

```
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #3 Information
-------------------------
Key Type              : Release (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #4 Information
-------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

Related Commands

命令	Description
show version	显示软件版本、硬件配置、许可证密钥和相关运行时间数据。

show ssd

要查看 SSD 的状态，请使用 **show ssd** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

show ssd

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示了有关 SSD 的信息：

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

Related Commands

命令	Description
configure raid	在 RAID 中添加或删除 SSD。
show raid	显示 RAID 状态。

show ssh-access-list

要显示管理接口的 SSH 访问列表设置，请使用 **show ssh-access-list** 命令。

show ssh-access-list

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

使用此命令可显示管理接口的 SSH 访问列表设置。访问列表确定用户可以从哪些 IP 地址尝试与管理 IP 地址建立 SSH 连接。此列表不控制对任何数据接口的 SSH 访问。

示例

以下示例是 **show ssh-access-list** 命令的默认输出。此访问列表允许从任何 IP 地址到管理 IP 地址的 SSH 连接。任何用户都必须提供有效的用户名/密码才能实际完成 SSH 连接。

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

Related Commands

命令	Description
configure ssh-access-list	配置管理接口的 SSH 访问列表。

show ssl

要显示有关活动 SSL 会话和可用密码的信息，请使用 **show ssl** 命令。

show ssl ［**cache** | **ciphers** ［*level*］ | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

Syntax Description

cache	（可选）显示 SSL 会话缓存统计信息。
ciphers	（可选）显示可用的 SSL 密码。包含 level 关键字以仅查看可用于给定级别的密码，这表示密码强度。以下是按强度递增的可能级别。 • **all** • **low** • **medium** （如果未指定级别，则为默认值） • **fips** • **high** （仅适用于 TLSv1.2）
errors [**trace**]	（可选）显示SSL错误。包括trace关键字，以包括每个错误的跟踪信息。
mib [**64**]	（可选）显示 SSL MIB 统计信息。包括 64 关键字以查看 64 位计数器统计信息。
objects	（可选）显示 SSL 对象统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关当前 SSLv3 或更高会话的信息，包括启用的密码顺序、禁用了哪些密码、正在使用的 SSL 信任点，以及是否启用证书身份验证。这些设置适用于数据接口上的 SSL 连接，而不是管理接口上的 SSL 连接。

示例

以下是 **show ssl** 命令的输出示例：

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
```

```
Certificate authentication is not enabled
```

以下是 **show ssl ciphers** 命令的输出示例。

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

```
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

show ssl-policy-config

要显示当前应用的 SSL 策略配置有关的信息，包括策略说明、默认日志记录设置、所有已启用的 SSL 规则和规则配置、受信任 CA 证书以及无法解密的流量操作，请使用 **show ssl-policy-config** 命令。

show ssl-policy-config

Command History

版本	修改
6.1	引入了此命令。

使用指南

在 管理中心 中配置 SSL 策略并将其附加到分配给设备的访问控制策略。您可以使用此命令查看有关为通过设备的流量进行 SSL 解密而配置的操作的信息。

示例

以下示例显示未为设备配置 SSL 策略时所显示的内容。

```
> show ssl-policy-config
SSL policy not yet applied.
```

以下示例显示已配置的 SSL 策略。

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                              thawte-Primary-Root-CA
                              UTN-DATACorp-SGC
                              Chambers-of-Commerce-Root-2008
                              Izenpe.com-1
                              A-Trust-Qual-02
                              A-Trust-nQual-03
                              Common-Policy
```

```
                                Starfield-Root-Certificate-Authority-G2
                                GeoTrust-Primary-Certification-Authority
                                Certum-Trusted-Network-CA
                                UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                CA-Disig-Root-R1
                                C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                Thawte-Server-CA-1
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G3
                                COMODO-Certification-Authority
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G5
                                UTN-USERFirst-Client-Authentication-and-Email
                                TC-TrustCenter-Universal-CA-III
                                Cisco-Root-CA-2048
                                Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

=============[ Undecryptable Actions ]==============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

Related Commands

命令	Description
show access-policy-config	显示有关当前配置的访问控制策略的信息。

show ssl-protocol

要显示当前为 HTTPS 访问本地设备管理器 () 而配置的 SSL 协议，请使用 设备管理器**show ssl-protocol** 命令。

show ssl-protocol

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看为管理接口配置的 SSL 协议。这些是 HTTPS 连接允许的协议，用于打开本地管理器 设备管理器。这些协议不用于远程管理器。

使用 **configure ssl-protocol** 命令配置这些协议。

示例

以下示例显示使用本地管理器时如何查看当前定义的 SSL 协议。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

Related Commands

命令	Description
configure ssl-protocol	配置用于 HTTPS 访问管理接口的 SSL 协议。

show startup-config

要显示启动配置或在启动配置加载时显示任何错误，请使用 **show startup-config** 命令。

show startup-config ［**errors**］

Syntax Description

errors	（可选）显示当加载启动配置时生成的任何错误。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show startup-config 命令可显示启动系统配置信息。您不能直接配置这些命令。相反，它们由控制设备的管理器配置，例如 管理中心 或 设备管理器。

但是，这是部分配置。它仅显示可使用 ASA 软件配置命令配置的内容，但某些命令可能特定于 threat defense。这些命令移植到 threat defense。因此，您应仅将启动配置中的信息用作故障排除辅助工具。使用设备管理器作为分析设备配置的主要方法。

示例

以下是 **show startup-config** 命令的输出示例：

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names

(...Output Truncated...)
```

Related Commands

命令	Description
show running-config	显示运行配置。

show summary

要显示有关设备的最常用信息（版本、类型、UUID 等）的摘要，请使用 **show summary** 命令。

show summary

Command History

版本	修改
6.1	引入了此命令。

使用指南

摘要信息包括基本 **show version** 输出以及应用的策略列表和 Snort 版本信息。

示例

以下是显示摘要信息的示例。

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
-----------------------------------------------------

------------------[ policy info ]--------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

-----------------------------------------------------

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
-----------------------------------------------------
```

show sunrpc-server active

要显示为 Sun RPC 服务打开的针孔，例如 NFS 和 NIS，请使用**show sunrpc-server active** 命令。

show sunrpc-server active

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show sunrpc-server active** 命令的输出示例：

```
> show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        ------------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

LOCAL 列中的条目显示内部接口上客户端或服务器的 IP 地址，而 FOREIGN 列中的值则显示外部接口上客户端或服务器的 IP 地址。

Related Commands

命令	Description
clear sunrpc-server active	清除为 Sun RPC 服务（如 NFS 或 NIS）开放的针孔。
show running-config sunrpc-server	显示有关 SunRPC 服务配置的信息。

show switch mac-address-table

要查看交换机 MAC 地址表，请使用 **show switch mac-address-table** 命令。

注释 仅支持 Firepower 1010。

show switch mac-address-table

Command History

版本	修改
6.5	引入了此命令。

使用指南

交换机 MAC 地址表为交换机硬件中的每个 VLAN 内的流量维护 MAC 地址到交换机端口的映射。网桥 MAC 地址表为 VLAN 之间传递的流量维护 MAC 地址到 VLAN 接口的映射。

MAC 地址条目的有效期为 5 分钟。

示例

以下是 **show switch mac-address-table** 命令的输出示例。

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
 Mac Address | VLAN | Type | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 | dynamic | 287 | Et1/1
 0012.d927.fb03 | 0001 | dynamic | 287 | Et1/1
 0013.c4ca.8a8c | 0001 | dynamic | 287 | Et1/1
 00b0.6486.0c14 | 0001 | dynamic | 287 | Et1/1
 00d0.2bff.449f | 0001 | static | - | In0/1
 0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

下表显示每个字段的说明：

表 *3: show switch mac-address-table* 字段

字段	Description
Mac Address	显示 MAC 地址。
VLAN	显示与 MAC 地址关联的 VLAN。
Type	显示 MAC 地址是动态获知、作为静态组播地址获知还是静态获知的。唯一的静态条目用于内部背板接口。
Age	显示 MAC 地址表中的动态条目的期限。

字段	Description
Port	显示用于通过 MAC 地址访问主机的交换机端口。

Related Commands

命令	Description
show switch vlan	显示 VLAN 和物理 MAC 地址关联。

show switch vlan

要查看 VLAN 和关联的交换机端口，请使用 **show switch vlan** 命令。

注释 仅支持 Firepower 1010。

show switch vlan

Command History

版本	修改
6.5	引入了此命令。

使用指南

此命令仅适用于具有内置交换机的型号。对于其他型号，请使用 **show vlan** 命令。

示例

以下是 **show switch vlan** 命令的输出示例。

```
> show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et1/1, Et1/2
200  outside                         up        Et1/8
300  -                               down      Et1/2, Et1/3
400  backup                          down      Et1/4
```

下表显示每个字段的说明：

表 *4: show switch vlan* 字段

字段	Description
VLAN	显示 VLAN 编号。
Name	显示 VLAN 接口的名称。如果未设置名称，或者没有 VLAN 接口，则显示屏会显示破折号 (-)。
Status	显示状态（up 或 down）以从/向交换机中的 VLAN 接收/发送流量。VLAN 中需要至少一个交换机端口处于 up 状态才能使 VLAN 处于 up 状态。
Ports	显示为每个 VLAN 分配的交换机端口。如果某个交换机端口为多个 VLAN 列出，则该端口是中继端口。上面的输出示例显示 Ethernet 1/2 是承载 VLAN 100 和 VLAN 300 的中继端口。

Related Commands

命令	Description
show switch mac-address-table	显示交换机 MAC 地址表。

show tcpstat

要显示 TCP 协议栈的状态以及在设备上终止的 TCP 连接（用于调试），请使用 **show tcpstat** 命令。

show tcpstat

Command History

版本	修改
6.1	引入了此命令。

使用指南

show tcpstat 命令可用于显示 TCP 堆栈和设备上终止的 TCP 连接的状态。下表介绍了所显示的 TCP 统计信息。

表 *5: Show tcpstat* 命令中的 *TCP* 统计信息

统计信息	Description
tcb_cnt	TCP 用户数。
proxy_cnt	TCP 代理数。TCP 代理被用户授权使用。
tcp_xmt pkts	TCP 堆栈发送的数据包数。
tcp_rcv good pkts	TCP 堆栈接收的良好数据包数。
tcp_rcv drop pkts	TCP 堆栈丢弃的已接收数据包数。
tcp bad chksum	校验和错误的已接收数据包数。
tcp user hash add	已添加到散列表的 TCP 用户数。
tcp user hash add dup	当尝试添加新用户时发现散列表中已存在 TCP 用户的次数。
tcp user srch hash hit	当搜索时在散列表中找到 TCP 用户的次数。
tcp user srch hash miss	当搜索时在散列表中未找到 TCP 用户的次数。
tcp user hash delete	从散列表中删除 TCP 用户的次数。
tcp user hash delete miss	当尝试删除 TCP 用户时在散列表中找不到该用户的次数。
lip	TCP 用户的本地 IP 地址。
fip	TCP 用户的外部 IP 地址。
lp	TCP 用户的本地端口。
fp	TCP 用户的外部端口。

统计信息	Description
st	TCP 用户的状态（请参阅 RFC 793）。可能值如下： 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP 用户的重新传输队列的长度。
inqlen	TCP 用户的输入队列的长度。
tw_timer	TCP 用户的 time_wait 计时器的值（以毫秒为单位）。
to_timer	TCP 用户的非活动超时计时器的值（以毫秒为单位）。
cl_timer	TCP 用户的关闭请求计时器的值（以毫秒为单位）。
per_timer	TCP 用户的持续计时器的值（以毫秒为单位）。
rt_timer	TCP 用户的重新传输计时器的值（以毫秒为单位）。
tries	TCP 用户的重新传输计数。

示例

以下示例展示如何显示 TCP 堆栈的状态：

```
> show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
```

```
tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0 tries 0
```

命令	Description
show conn	显示使用的连接和可用的连接。

show tech-support

要显示由技术支持分析师用于诊断的信息，请使用 **show tech-support** 命令。

show tech-support

Command History

版本	修改
6.1	引入了此命令。
7.1	添加了 **show access-list element-count** 和 **show asp rule-engine** 的输出。

使用指南

show tech-support 命令可列出技术支持分析师帮助您诊断问题时所需的信息。

示例

以下示例展示如何显示用于技术支持分析的信息。输出已缩短，仅显示其开头。输出非常长，需要很长时间才能浏览结果。

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

show threat-detection memory

要显示由运行配置中的 **threat-detection statistics** 命令启用的高级威胁检测统计信息使用的内存，请使用 **show threat-detection memory** 命令。

show threat-detection memory

Command History

版本	修改
6.3	引入了此命令。

使用指南

某些统计可使用大量内存，并会影响系统性能。此命令可监控内存使用情况，以便您在必要时调整配置。

使用 FlexConfig 配置 **threat-detection statistics** 命令。

示例

以下是 **show threat-detection memory** 命令的输出示例：

```
> show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks               70265072


Regular memory                BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888


Total TD memory:                 70460960
```

命令	Description
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics port	显示端口统计信息。

命令	Description
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。

show threat-detection rate

使用 **threat-detection basic-threat** 命令（使用 FlexConfig）启用基本威胁检测时，可以使用 **show threat-detection rate** 命令查看统计信息。

show threat-detection rate ［**min-display-rate** *events_per_second*］［**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**］

Syntax Description

acl-drop	（可选）显示由于访问列表拒绝而产生丢弃数据包的速率。
bad-packet-drop	（可选）显示由于数据包格式错误（如 invalid-ip-header 或 invalid-tcp-hdr-length）而被拒绝所产生丢弃数据包的速率。
conn-limit-drop	（可选）显示由于超过连接限制（系统范围的资源限制和配置中设置的限制）而产生丢弃数据包的速率。
dos-drop	（可选）显示由于检测到 DoS 攻击（如无效的 SPI，状态防火墙检查失败）而产生丢弃数据包的速率。
fw-drop	（可选）显示由于基本防火墙检查失败而产生丢弃数据包的速率。此选项是包括此命令中所有防火墙相关数据包丢弃的组合速率。它不包括非防火墙相关丢包（例如 interface-drop、inspect-drop 和 scanning-threat）。
icmp-drop	（可选）显示由于检测到可疑 ICMP 数据包而被拒绝所产生丢弃数据包的速率。
inspect-drop	（可选）显示由于数据包导致应用检查失败而产生丢弃数据包的速率限制。
interface-drop	（可选）显示由于接口过载而产生丢弃数据包的速率限制。
min-display-rate *events_per_second*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位， 0 - 2147483647）的统计信息。
scanning-threat	（可选）显示由于检测到扫描攻击而产生丢弃数据包的速率。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。例如，完整扫描威胁检测采用此扫描攻击频率信息，通过将主机分类为攻击者并自动避开这些主机，从而根据此信息采取行动。
syn-attack	（可选）显示由于会话不完整（如 TCP SYN 攻击或无返回数据 UDP 会话攻击）而产生丢弃数据包的速率。

Command History

版本	修改
6.3	引入了此命令。

使用指南

显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。
- 超过速率的次数。
- 固定时间段内的事件总数。

系统会在平均速率间隔内计算30次事件计数，换句话说，系统在每个突发周期的末尾检查速率，总共检查30个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 10 分钟，则突发间隔为 10 秒。如果上一个突发间隔为 3:00:00 至 3:00:10，并且您在 3:00:15 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 59 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection rate** 命令的输出示例：

```
> show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
10-min ACL  drop:                  0               0       0                   16
1-hour ACL  drop:                  0               0       0                  112
1-hour SYN attck:                  5               0       2                21438
10-min  Scanning:                  0               0      29                  193
1-hour  Scanning:                106               0      10               384776
1-hour Bad  pkts:                 76               0       2               274690
10-min  Firewall:                  0               0       3                   22
1-hour  Firewall:                 76               0       2               274844
10-min DoS attck:                  0               0       0                    6
1-hour DoS attck:                  0               0       0                   42
10-min Interface:                  0               0       0                  204
1-hour Interface:                 88               0       0               318225
```

Related Commands

命令	Description
clear threat-detection rate	清除基本威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics	显示威胁检测统计信息。

show threat-detection scanning-threat

如果使用 **threat-detection scanning-threat** 命令启用扫描威胁检测（使用 FlexConfig），则使用 **show threat-detection scanning-threat** 命令查看归类为攻击者和目标的主机。

show threat-detection scanning-threat ［**attacker** | **target**］

Syntax Description

attacker	（可选）显示攻击主机 IP 地址。
target	（可选）显示目标主机 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show threat-detection scanning-threat** 命令的输出示例：

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

Related Commands

命令	Description
clear threat-detection scanning-threat	清除扫描威胁攻击者和目标的列表。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics	显示威胁检测统计信息。
shun	阻止来自指定主机的连接，例如扫描威胁攻击者。

show threat-detection shun

如果使用 **threat-detection scanning-threat** 命令（使用 FlexConfig）启用扫描威胁检测，并自动避开攻击主机，则使用 **show threat-detection shun** 命令查看当前避开的主机。

show threat-detection scanning-host

Command History

版本	修改
6.3	引入了此命令。

使用指南

要释放回避的主机，请使用 **clear threat-detection shun** 命令。

示例

以下是 **show threat-detection shun** 命令的输出示例：

```
> show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

Related Commands

命令	Description
clear threat-detection shun	清除自动避开的主机列表。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection scanning-threat	显示扫描威胁攻击者和目标。
show threat-detection statistics	显示威胁检测统计信息。
shun	阻止来自指定主机的连接，例如扫描威胁攻击者。

show threat-detection statistics

如果使用 **threat-detection statistics** 命令（使用 FlexConfig）启用威胁统计信息，请使用 **show threat-detection statistics** 命令查看统计信息。为清楚起见，下图中分别显示了主要关键字和选项。

show threat-detection statistics ［**min-display-rate** *eps*］ **host** ［*ip_address* ［*mask*］］

show threat-detection statistics ［**min-display-rate** *eps*］ **port** ［*start_port*［*-end_port*］］

show threat-detection statistics ［**min-display-rate** *eps*］ **protocol** ［*number* | *name*］

show threat-detection statistics ［**min-display-rate** *EPS*］ **top** ［**access-list** | **host** | **port-protocol**］［**rate-1** | **rate-2** | **rate-3**］ | **tcp-intercept** ［**all**］［**detail**］［**long**］］

Syntax Description

host [*ip_address* [*mask*]]	显示主机统计信息。您可以选择指定 IP 地址以显示特定主机的统计信息。可以包括主机的子网掩码。 通过使用 FlexConfig 配置 **threat-detection statistics host** 命令来启用主机统计信息。
min-display-rate *eps*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位， 0 - 2147483647）的统计信息。
port [*start_port*[*-end_port*]]	显示 TCP/UDP 端口统计信息。您可以选择指定一个端口或一系列端口，范围介于 0 和 65535 之间。 通过使用 FlexConfig 配置 **threat-detection statistics port** 命令来启用端口统计信息。
protocol [*number* | *name*]	显示协议统计信息。您可以选择按编号或名称指定协议。数字可以是 0 - 255。名称可以是下列项目之一：ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、pim、pptp、snp、tcp、udp。 通过使用 FlexConfig 配置 **threat-detection statistics protocol** 命令来启用协议统计信息。

top [**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**]	根据启用统计信息的选项，显示前 10 个访问规则、主机和端口/协议。您可以使用以下关键字缩小视图范围： • **access-list** 显示与数据包匹配的前 10 名 ACE，包括允许和拒绝 ACE。如果使用 **threat-detection basic-threat** 命令启用基本威胁检测，则可以使用 **show threat-detection rate access-list** 命令跟踪访问列表拒绝。 • **host** 显示每个固定时间段的前 10 名主机统计信息。由于威胁检测算法的原因，用于故障转移链路或状态链路的接口可能显示为前 10 名主机之一。当将一个接口同时用于故障转移和状态链路时，更有可能出现这种情况。这是预期行为，您可以在显示中忽略此 IP 地址。 • **port-protocol** 显示 TCP/UDP 端口和 IP 协议类型的前 10 名合并统计信息。TCP（协议 6）和 UDP（协议 17）未包含在 IP 协议的显示内容中。 • **rate-1**、 **rate-2**、 **rate-3** 仅显示指定固定速率周期的统计信息，其中 1 表示最小间隔，3 表示最大间隔。例如，如果显示最近 1 小时、8 小时和 24 小时的统计信息，则速率 1 为 1 小时，速率 2 为 8 小时，速率 3 为 24 小时。
top tcp-intercept [**all**] [**detail**] [**long**]	显示 TCP 拦截统计信息。显示内容包含受到攻击的前 10 台受保护服务器。可以包括以下关键字： • **all** 显示所有被跟踪服务器的历史数据。 • **detail** 显示历史采样数据。 • **long** 以长格式显示统计历史记录，其中包含服务器的实际 IP 地址和转换后的 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

使用指南

威胁检测统计信息显示允许和丢弃的流量速率。

显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

系统会在平均速率间隔内计算30次事件计数，换句话说，系统在每个突发周期的末尾检查速率，总共检查30个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率

间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

下表说明了除 TCP 拦截视图之外的所有命令的输出。有关该输出的说明，请参阅 TCP 拦截示例。

字段	Description
Top Name, ID	对于排名靠前的报告，此列显示访问控制条目的名称或编号、主机的 IP 地址或端口或协议的名称/ID 编号。 条目按固定速率间隔分组，并在时间段内排名，从 [0]（最高计数）到 [9]（最低计数）。对于所有 10 个位置，您可能没有足够的统计信息，因此在给定时间间隔内显示的项目可能少于 10 个。 对于主机和端口协议，按固定间隔发送和接收的字节和数据包进行分组。
Average(eps)	显示每个时间段内的平均速率（单位：事件数/秒）。 系统在每个突发时段结束时，为共计 30 个已完成突发间隔存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 show 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）对于 Average(eps) 说明中指定的示例，当前速率为 3:19:30 至 3:20:00 的速率
触发器	显示超出丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

字段	Description
条目标题	统计信息按标题下的固定间隔分组。标题可以包括以下各行中解释的信息。通常，条目标题以以下内容开头： • 带有主机 IP 地址的主机。 • 端口号/名称。例如，80/HTTP。 • 协议编号或名称。例如，ICMP。 • 对于排名靠前的报告，为固定间隔和统计信息类型。对于访问列表，标题表示这是针对 ACL 命中的。
tot-ses	显示自主机、端口或协议添加到数据库后的该主机会话总数。
act-ses	显示主机、端口或协议当前参与的活动会话总数。
fw-drop (Host only.)	显示防火墙丢弃数。防火墙丢包是一个组合速率，其中包括在基本威胁检测中跟踪的与防火墙有关的所有丢包，包括访问列表拒绝的数据包、错误数据包、超出连接限制的数据包、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包以及无返回数据 UDP 会话攻击数据包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
insp-drop (Host only.)	显示因为数据包未通过应用检查而被丢弃的数据包的数量。
null-ses (Host only.)	显示空会话数量，空会话是指在 30 秒超时内未完成的 TCP SYN 会话，以及在会话开始后 3 秒内没有其服务器发送的任何数据的 UDP 会话。
bad-acc (Host only.)	显示对处于关闭状态的主机端口的不良访问尝试次数。当确定某个端口处于空会话时（请参阅上文），该主机的端口状态设置为 HOST_PORT_CLOSE。任何访问该主机端口的客户端都会被立即分类为错误访问，无需等待超时。
20-min, 1-hour, 8-hour, and 24-hour	显示这些固定速率间隔的统计信息。 • Sent byte, sent pkts - 显示从主机、端口或协议成功发送的字节数或数据包数。 • Sent drop - 显示已从主机、端口或协议发送但因为是扫描攻击的一部分而被丢弃的数据包数。 • Recv byte, pkts - 显示主机、端口或协议成功接收的字节数或数据包数。 • Sent drop - 显示已从主机、端口或协议发送但因为是扫描攻击的一部分而被丢弃的数据包数。

示例

以下是 **show threat-detection statistics host** 命令的输出示例：

```
> show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938              0       0             10580308
  8-hour Sent byte:                367              0       0             10580308
 24-hour Sent byte:                122              0       0             10580308
  1-hour Sent pkts:                 28              0       0               104043
  8-hour Sent pkts:                  3              0       0               104043
 24-hour Sent pkts:                  1              0       0               104043
  20-min Sent drop:                  9              0       1                10851
  1-hour Sent drop:                  3              0       1                10851
  1-hour Recv byte:               2697              0       0              9712670
  8-hour Recv byte:                337              0       0              9712670
 24-hour Recv byte:                112              0       0              9712670
  1-hour Recv pkts:                 29              0       0               104846
  8-hour Recv pkts:                  3              0       0               104846
 24-hour Recv pkts:                  1              0       0               104846
  20-min Recv drop:                 42              0       3                50567
  1-hour Recv drop:                 14              0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0              0       0                  614
  8-hour Sent byte:                  0              0       0                  614
 24-hour Sent byte:                  0              0       0                  614
  1-hour Sent pkts:                  0              0       0                    6
  8-hour Sent pkts:                  0              0       0                    6
 24-hour Sent pkts:                  0              0       0                    6
  20-min Sent drop:                  0              0       0                    4
  1-hour Sent drop:                  0              0       0                    4
  1-hour Recv byte:                  0              0       0                  706
  8-hour Recv byte:                  0              0       0                  706
 24-hour Recv byte:                  0              0       0                  706
  1-hour Recv pkts:                  0              0       0                    7
```

以下是 **show threat-detection statistics port** 命令的输出示例：

```
> show threat-detection statistics port

                        Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

以下是 **show threat-detection statistics protocol** 命令的输出示例：

```
> show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

以下是 **show threat-detection statistics top access-list** 命令的输出示例：

```
> show threat-detection statistics top access-list

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
  8-hour ACL hits:
              100/3[0]              21            1298       0               623488
              200/2[1]               5             326       0               156786
              100/1[2]               5             326       0               156786
```

以下是 **show threat-detection statistics top port-protocol** 命令的输出示例：

```
> show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
 3         gopher   69              65               0       0          24345678
 4    Protocol-96 * 96              63               0       0          22345678
 5      Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7     Port-8191-65535              55               0       0          12345678
 8           SMTP  366              34               0       0           3345678
 9         IPinIP *  4              30               0       0           2345678
10          EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

以下是 **show threat-detection statistics top host** 命令的输出示例：

```
> show threat-detection statistics top host

                    Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938               0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28               0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9               0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697               0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29               0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42               0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367               0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3               0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3               0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337               0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3               0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14               0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122               0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1               0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112               0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1               0       0               104846
```

以下是 **show threat-detection statistics top tcp-intercept** 命令的输出示例：

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

下表对 TCP 截取输出进行了解释。

字段	Description
Monitoring window size	显示系统采样统计信息的时间段。默认值为 30 分钟。您可以使用 FlexConfig 的 **threat-detection statistics tcp-intercept rate-interval** 命令更改此设置。系统在此间隔内采样 30 次数据。
Sampling interval	显示采样的间隔。此值始终为速率间隔除以 30。
Rank	显示排名 1 到 10，其中 1 是最受攻击的服务器，10 是最不受攻击的服务器。
Server IP:Port	显示正受到攻击的服务器 IP 地址和端口。
Interface	显示服务器受到攻击的接口。
Ave Rate	显示采样期间内的平均攻击速率（以攻击数/秒为单位）。
Cur Rate	显示当前攻击速率（以攻击数/秒为单位）。
Total	显示攻击总数。
Source IP	显示攻击者 IP 地址。
Last Attack Time	显示上一次攻击发生的时间。

以下是 **show threat-detection statistics top tcp-intercept long** 命令的输出示例，括号中为实际服务器 IP 地址：

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source
 IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

以下显示 **show threat-detection statistics top tcp-intercept detail** 命令的输出示例，这显示采样数据。采样数据显示 30 个采样周期中每个周期的攻击次数。

```
> show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
```

```
--------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (30 Samplings):
              95348       95337       95341       95339       95338       95342
              95337       95348       95342       95338       95339       95340
              95339       95337       95342       95348       95338       95342
              95337       95339       95340       95339       95347       95343
              95337       95338       95342       95338       95337       95342
              95348       95338       95342       95338       95337       95343
              95337       95349       95341       95338       95337       95342
              95338       95339       95338       95350       95339       95570
              96351       96351       96119       95337       95349       95341
              95338       95337       95342       95338       95338       95342
......
```

Related Commands

命令	Description
clear threat-detection statistics	清除威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。

show time

要显示设备的 UTC 和本地时间和日期，请使用 **show time** 命令。

show time

Command History

版本	修改
6.0.1	引入了此命令。

示例

以下是 **show time** 命令的输出示例。

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

show time-range

要显示所有时间范围对象的配置，请使用 **show time-range** 命令。

注释 此命令不显示设备时间。要查看设备时间，请使用 显示时间。

show time-range timezone ［ 名称 ］

Syntax Description

name	（可选）仅显示此时间范围对象的信息。
timezone	要查看为时间范围策略配置的时区，请使用时区。

Command History

版本	修改
6.3	引入了此命令。
6.6	添加了时区关键字。

示例

此示例显示如何显示时间范围对象的配置。在本示例中，有一个名为 work-hours 的对象。非活动意味着对象未被使用。

```
> show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

以下是 **show time-range timezone** 命令的输出示例：

```
> show time-range timezone
Time-range Clock:
------------------------------
13:20:22.852 tzname Tue Aug 18 2020
```

show tls-proxy

要显示加密检测的 TLS 代理和会话信息，请使用 **show tls-proxy** 命令。

show tls-proxy [*tls_name* | **session** [**host** *host_address* | **detail** [**cert-dump**] | **count** | **statistics**]]

Syntax Description

count	仅显示会话计数器。
detail [**cert-dump**]	显示详细 TLS 代理信息，包括每个 SSL 段和 LDC 的密码。添加 **cert-dump** 关键字以获取本地动态证书 (LDC) 的十六进制转储。 您还可以将这些关键字与 **host** 选项配合使用。
host *host_address*	指定特定主机的 IPv4 或 IPv6 地址，以显示关联的会话。
session	显示活动 TLS 代理会话。
statistics	显示监控和管理 TLS 会话的统计信息。
tls_name	要显示的 TLS 代理的名称。

Command History

版本	修改
6.3	引入了此命令。

使用指南

您可以使用此命令查看的 TLS 代理是仅为加密应用检测配置的代理。它们适用于 SIP、SCCP (Skinny) 或 Diameter 检测。这些 TLS 代理与 SSL 解密或 VPN 策略无关。

示例

以下是 **show tls-proxy** 命令的输出示例：

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
      Server proxy:
            Trust-point: local_ccm
      Client proxy:
            Local dynamic certificate issuer: ldc_signer
            Local dynamic certificate key-pair: phone_common
            Cipher-suite <unconfigured>
      Run-time proxies:
            Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
                  Active sess 1, most sess 4, byte 3244
```

以下是 **show tls-proxy session** 命令的输出示例：

```
> show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

以下是 **show tls-proxy session detail** 命令的输出示例：

```
> show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
      Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1

      Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
      Status: Available
      Certificate Serial Number: 29
      Certificate Usage: General Purpose
      Public Key Type: RSA (1024 bits)
      Issuer Name:
             cn=TLS-Proxy-Signer
      Subject Name:
             cn=SEP0002B9EB0AAD
             o=Cisco Systems Inc
             c=US
      Validity Date:
            start date: 00:47:12 PDT Feb 27 2007
            end   date: 00:47:12 PDT Feb 27 2008
      Associated Trustpoints:
```

以下是 **show tls-proxy session statistics** 命令的输出示例：

```
> show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                        0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                             2
    SCCP:                                           20
    DIAMETER:                                      200
Total TLS Proxy Sessions
    Established:                                   822
    Platform Limit:                               1000
```

show track

要显示有关安全级别协议 (SLA) 跟踪流程跟踪的对象的信息，请使用 **show track** 命令。

show track ［*track-id*］

Syntax Description

track-id	跟踪条目对象 ID 编号，范围为 1 到 500。

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show track** 命令的输出示例：

```
> show track

Track 5
      Response Time Reporter 124 reachability
      Reachability is UP
      2 changes, last change 03:41:16
      Latest operation return code: OK
      Tracked by:
                 STATIC-IP-ROUTING 0
```

show traffic

要显示接口传输和接收活动，请使用 **show traffic** 命令。

show traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

show traffic 命令列出了自上次输入 **show traffic** 命令以来或设备上线以来通过每个接口的数据包和字节数。秒数是设备自上次重启以来的在线持续时间，除非自上次重启以来输入过 **clear traffic** 命令。如果是这种情况，则秒数是自输入命令以来的持续时间。

统计信息首先根据接口名称显示。在指定接口之后，将根据物理接口显示统计信息。接口可以包括系统用于内部通信的隐藏虚拟接口。

示例

以下是 **show traffic** 命令的简短输出示例，显示单个接口的统计信息。每个接口显示相同的统计信息。

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

Related Commands

命令	Description
clear traffic	重置用于发送和接收活动的计数器。

show upgrade

要显示有关系统软件升级的信息，请使用 **show upgrade** 命令。

show upgrade { **revert-info** | **status** [**detail**] [**continuous**] }

Syntax Description

revert-info	显示您可以恢复使用的系统版本（如果有任何版本可用于恢复）。如果没有可用的恢复版本，则无法使用 **upgrade revert** 命令。
status	显示升级的状态。可以包含以下可选关键字： • **detail** 除摘要状态信息外，还显示升级日志。 • **continuous** 显示生成的升级消息。您可以单独使用此关键字，也可以将其与detail关键字结合使用。

Command History

版本	修改
6.7	引入了此命令。

使用指南

可能的状态包括：

- 未在进行升级。
- 正在进行主要升级。
- 正在进行补丁升级。
- 正在进行修复程序。
- 主要升级失败。运行 “cancel” 进行恢复。

  重新启动可能会发生，也可能不会发生，具体取决于升级失败阶段。
- 主要升级失败。重新启动设备以进行恢复。

示例

以下示例显示当前正在进行的升级的状态。要查看已完成升级的状态，请使用 **show last-upgrade status** 命令。

```
> show upgrade status
Upgrade from 6.3.0 to 6.7.0 in progress (11% progress, time remaining 8 mins)
Time started: Tue Dec  3 23:50:31 UTC 2020
Current state: Tue Dec  3 23:51:01 UTC 2020 Running script 200_pre/001_check_reg.pl...
```

以下示例显示恢复信息。在本示例中，确实存在您可以恢复的版本。如果没有可用的版本，则消息为“没有可用于恢复的版本”。

```
> show upgrade revert-info
You can revert to version 6.4.0-102
at 2020-03-20T22:49:43+0000

It uses 4946MB of disk space.

Version 6.4.0-102 is available for revert.
```

Related Commands

命令	Description
show last-upgrade status	显示有关上次系统软件升级的信息。
upgrade	取消、恢复或重试系统软件升级。

show user

要显示用于访问设备上的命令行接口 (CLI) 的用户账号，请使用 **show user** 命令。

show user ［*username1* ［*usernam2*］［...］］

Syntax Description

username1 [*usernam2*] [...]	（可选。）一个或多个空格分隔的用户名。如果不指定任何名称，则会显示所有用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

系统将为每个用户显示以下信息。使用 **configure user add** 命令创建用户账号。

- Login - 登录名。
- UID - 数字用户 ID。
- Auth - 如何对用户进行身份验证，本地或远程（通过目录服务器）。
- Access — 用户的权限级别，基础或配置。使用 **configure user access** 命令更改其设置。
- 已启用 - 用户是否处于活动状态，已启用或已禁用。使用 **configure user enable**/**disable** 命令更改此设置。
- Reset - 用户下次登录时是否必须更改账户密码，是或否。使用 **configure user forcereset** 命令更改此设置。
- Exp- 还剩下多少天必须更改用户密码。从不表示密码不会过期。使用 **configure user aging** 命令更改其设置。
- Warn - 在密码到期前警告用户更改密码的天数。N/A 表示警告不适用。使用 **configure user aging** 命令更改其设置。
- 宽限期 - 宽限期，即密码到期后用户可以更改的天数。禁用意味着没有宽限期。宽限期仅适用于运行 FXOS 的设备。使用 **configure user aging** 命令更改其设置。
- Str - 用户密码是否必须符合强度检查标准，Dis (禁用) 或 Ena (启用)。使用 **configure user strengthcheck** 命令配置此选项。
- Lock - 用户账户是否因登录失败太多次而被锁定，是或否。使用 **configure user unlock** 命令以解锁用户账号。
- Max - 用户账户被锁定前允许的最多登录失败次数。N/A 表示永远无法锁定账户。使用 configure user maxfailedlogins 命令更改此设置。

示例

以下示例显示如何显示为 CLI 访问定义的用户。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

以下示例包括外部用户和宽限期。

```
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

命令	Description
configure user add	添加用于 CLI 访问的用户账号。

show version

要显示硬件型号、软件版本、UUID、入侵规则更新版本和 VDB 版本，请使用 **show version** 命令。

show version ［**detail** | **system**］

Syntax Description

detail	**show version** 和 **show version detail** 显示相同的信息。
system	此关键字将其他系统信息附加到 **show version**显示的信息。

Command History

版本	修改
6.1	引入了此命令。
7.1	有关启动（引导）系统所需时间的信息已添加到输出中。

使用指南

show version 命令和 **show version detail** 命令显示相同的基本系统信息。 **show version system** 命令显示此信息以及其他系统信息，例如自上次重新启动以来的运行时间和更具体的硬件信息。

示例

以下示例显示了 **show version** 的基础输出：

```
> show version
-------------------[ firepower ]--------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.2.0 (Build 1405)
UUID : 78ddf634-3754-11ec-87dd-ace5f9ec4cdc
Rules update version : 2022-01-11-001-vrt
LSP version : lsp-rel-20220111-1030
VDB version : 348
----------------------------------------------------
```

show version system 命令的以下示例输出附加了与 **show version** 命令相同的输出以及其他信息。

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 36 days 21 hours
```

```
Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type                : Release
Key Version               : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

从版本 7.1 开始，您可以看到启动系统所需的时间。该信息位于系统运行时间的状态之后。

```
> show version system
----------------------[ ftdv1 ]-----------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.1.0
(Build 1519)
UUID                      : b964ed5e-92c0-11eb-aaa2-cfab359c2436
LSP version               : lsp-rel-20210310-2255
VDB version               : 338
------------------------------------------------------

Cisco Adaptive Security Appliance Software Version 99.17(1)135
SSP Operating System Version 82.11(1.277i)

Compiled on Thu 25-Mar-21 00:49 GMT by builders
System image file is "boot:/asa99171-135-smp-k8.bin"
Config file at boot was "startup-config"

ftdv1 up 6 days 22 hours
Start-up time 5 secs

(remaining output redacted)
```

show vlan

要显示 threat defense 设备上配置的所有 VLAN，请使用 **show vlan** 命令。

show vlan ［**mapping** ［*primary_id*］］

Syntax Description

mapping	（可选）显示映射到主 VLAN 的辅助 VLAN。
primary_id	（可选）显示特定主 VLAN 的辅助 VLAN。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示已配置的 VLAN：

```
> show vlan
10-11,30,40,300
```

以下示例显示映射到每个主 VLAN 的辅助 VLAN：

```
> show vlan mapping
Interface                       Secondary VLAN ID                    Mapped VLAN ID
0/1.100                         200                                             300
0/1.100                         201                                             300
0/2.500                         400                                             200
```

Related Commands

命令	Description
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行时间状态和统计信息。

show vm

要显示 threat defense virtual 设备上的虚拟平台信息，请使用 **show vm** 命令。

show vm

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何显示有关 VMware 的信息：

```
> show vm

Virtual Platform Resource Status
--------------------------------
Number of vCPUs           :  4
Processor Memory          :  8192 MB
Hypervisor                :  VMware
```

show vpdn

要显示虚拟专用拨号网络 (VPDN) 连接（例如 PPPoE 或 L2TP）的状态，请使用 **show vpdn** 命令。

show vpdn {**group** *name* | **pppinterface id** *number* | **session** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **window**} | **tunnel** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **summary** | **transport**} | **username** *name*}

Syntax Description

group *name*	显示 VPDN 组配置。
id *number*	（可选）显示有关具有指定 ID 的 VPDN 会话的信息。
l2tp	（可选）显示有关 L2TP 的会话或隧道信息。
packets	显示会话或隧道数据包信息。
pppinterface	显示 PPP 接口信息。
pppoe	（可选）显示有关 PPPoE 的会话或隧道信息。
session	显示会话信息。
state	显示会话或隧道状态信息。
summary	显示隧道摘要。
transport	显示隧道传输信息。
tunnel	显示隧道信息。
username *name*	显示用户信息。
window	显示会话窗口信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可对 VPDN PPPoE 或 L2TP 连接进行故障排除。

示例

以下是 **show vpdn session** 命令的输出示例：

```
> show vpdn session
```

```
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

以下是 **show vpdn tunnel** 命令的输出示例：

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
```

show vpn load-balancing

请勿使用此命令。它与 threat defense不支持的功能相关。

show vpn-sessiondb

要显示有关 VPN 会话的信息，请使用以下 **show vpn-sessiondb** 命令之一。

show vpn-sessiondb ［**detail**］［**full**］｛**anyconnect** | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec**｝［**filter** *criteria*］［**sort** *criteria*］
show vpn-sessiondb ［**detail**］［**full**］ **index** *indexnumber*
show vpn-sessiondb failover
show vpn-sessiondb ospfv3 ［**filter ipaddress** *IP_address*］［**sort ipaddress**］

Syntax Description

anyconnect	显示 AnyConnect VPN 客户端会话。
detail	（可选）显示会话的相关扩展详细信息。例如，detail 选项用于 IPsec 会话，会显示其他详细信息，例如 IKE 散列算法、身份验证模式和再生密钥时间间隔。 如果您选择 detail 和 full 选项，则 threat defense 设备以机器可读格式显示详细输出。
failover	显示故障转移 IPsec 隧道的会话信息。
filter *filter_criteria*	（可选）根据指定的过滤器选项过滤输出。有关选项列表，请参阅使用指南部分。
full	（可选）显示流式未截断输出。在记录之间用 | 字符和 || 字符串对输出进行分段。
index *indexnumber*	按索引编号显示单个会话。指定会话的索引编号（范围为 1 - 65535）。
l2l	显示 VPN LAN-to-LAN 会话信息。
ospfv3	显示 OSPFv3 会话信息。
ra-ikev1-ipsec	显示 IPsec IKEv1 会话。
ra-ikev2-ipsec	显示 IKEv2 远程访问客户端连接的详细信息。
sort *sort_criteria*	（可选）根据您指定的排序选项将输出排序。有关选项列表，请参阅使用指南部分。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用以下选项对会话显示进行过滤和排序：可以过滤和排序的值因列出的会话类型而异。

Filter/Sort 选项	Description
filter a-ipaddress *IP_address*	过滤输出以仅显示指定的分配 IP 地址的信息。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
sort a-ipaddress	按分配的 IP 地址排序显示。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter a-ipversion {**v4** | **v6**}	过滤输出，仅显示已分配 IPv4 或 IPv6 地址的会话。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter encryption *encryption_algorithm*	过滤输出以仅显示使用指定加密算法的会话的信息。使用 ? 查看可用的方法。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
sort encryption	按会话中使用的加密算法对输出进行排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
filter inactive	过滤空闲和可能失去连接（由于休眠、移动设备断开连接等等）的非活动会话。从 threat defense 设备发送 TCP 保持连接而没有收到来自 AnyConnect 客户端的响应时，非活动会话数量会增长。用 SSL 隧道丢弃时间为每个会话加上时间戳。如果会话主动通过 SSL 隧道传输流量，则显示 00:00m:00s。 配合使用： **anyconnect** 注释 threat defense 设备不会将 TCP 保持连接发送到一些设备（例如 iPhone、iPad 和 iPod）以延长电池续航时间，因此故障检测无法区分断开连接与休眠。因此，按照设计，非活动状态计数器将保持为 00:00:00。
sort inactivity	将非活动会话排序。 配合使用： **anyconnect**
filter ipaddress *IP_address*	过滤输出以仅显示内部分配 IP 地址的信息。 配合使用： **l2l**、 **ospfv3**
sort ipaddress	按内部 IP 地址将显示排序。 配合使用： **l2l**、 **ospfv3**
filter ipversion {**v4** | **v6**}	过滤输出，仅显示源自具有 IPv4 或 IPv6 地址的终端的会话。 配合使用： **l2l**
filter name *username*	过滤输出以显示指定用户名的会话。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**

Filter/Sort 选项	Description
sort name	按用户名的字母顺序将显示排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
filter p-ipaddress *IP_address*	过滤输出以仅显示公共外部分配 IP 地址的信息。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
sort p-ipaddress	按公共外部 IP 地址对显示内容进行排序。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter p-ipversion {**v4** | **v6**}	过滤输出，仅显示来自具有公共 IPv4 或 IPv6 地址的终端的会话。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter protocol *name*	过滤输出以仅显示使用指定协议的会话的信息。使用 ? 查看可用的协议。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
sort protocol	按协议将显示排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**

下表对可能看到的输出字段进行了解释。

字段	Description
Auth Mode	用于身份验证该会话的协议或模式。
Bytes Rx	系统从远程对等设备或客户端接收的字节总数。
Bytes Tx	系统传输到远程对等设备或客户端的字节数。
Client Type	在远程对等设备上运行的客户端软件（如果可用）。
Client Ver	在远程对等设备上运行的客户端软件的版本。
Connection	连接或专用 IP 地址的名称。
D/H Group	Diffie-Hellman 组。用于生成 IPsec SA 加密密钥的算法和密钥大小。
Duration	会话登录时间与上次屏幕刷新之间的已用时间 (HH:MM:SS)。
EAPoUDP Session Age	上次成功的状态验证以来的秒数。
Encapsulation	用于应用 IPsec ESP（封装安全负载协议）加密和身份验证的模式（即，应用了 ESP 的原始 IP 数据包的一部分）。
Encryption	此会话使用的数据加密算法（如果有）。
EoU Age (T)	EAPoUDP Session Age 上次成功的状态验证以来的秒数。

字段	Description
Filter Name	指定的用来限制会话信息显示的用户名。
Hashing	用于创建数据包的散列的算法，该算法用于 IPsec 数据身份验证。
Hold Left (T)	Hold-Off Time Remaining. 如果上一状态验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
剩余的延缓时间	如果上一状态验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
IKE Neg Mode	用于交换密钥信息和设施 SA 的 IKE（IPsec 阶段 1）模式：积极或主要。
IKE Sessions	IKE（IPsec 阶段 1）会话数；通常为 1。这些会话为 IPsec 流量建立隧道。
Index	此记录的唯一标识符。
IP Addr	为此会话分配给远程客户端的专用 IP 地址。这也称为“内部”或“虚拟”IP 地址。它允许客户端在专用网络中显示为主机。
IPsec Sessions	IPsec（阶段 2）会话数，即通过隧道的数据流量会话。每个 IPsec 远程访问会话可以有两个 IPsec 会话：一个包含隧道终端，而另一个包含可通过隧道访问的专用网络。
License Information	显示关于共享 SSL VPN 许可证的信息。
Local IP Addr	分配给隧道本地终端（这是系统上的接口）的 IP 地址。
Login Time	会话登录的日期和时间 (MMM DD HH:MM:SS)。时间以 24 小时制显示。
NAC Result	网络准入控制状态验证的状态。它可以是下列类型之一： • Accepted - ACS 已成功验证远程主机的终端安全评估。 • Rejected - ACS 未能成功验证远程主机的终端安全评估。 • Exempted - 根据 threat defense 设备上配置的 Posture Validation Exception 列表，远程主机已被豁免终端安全评估验证。 • Non-Responsive - 远程主机没有响应 EAPoUDP Hello 消息。 • Hold-off - threat defense 设备在终端安全评估验证成功后丢失与远程主机的 EAPoUDP 通信。 • N/A - 根据 VPN NAC 组策略，已为远程主机禁用 NAC。 • Unknown - 终端安全评估验证正在进行中。
NAC Sessions	网络准入控制（EAPoUDP）会话数。
Packets Rx	系统从远程对等设备接收的数据包的数量。

字段	Description
Packets Tx	系统传输到远程对等设备的数据包数。
PFS Group	完全转发保密组编号。
Posture Token	访问控制服务器上可配置的信息文本字符串。ACS将安全评估令牌下载至系统，以实现协助系统监控、报告、调试和记录的参考用途。典型的安全评估令牌标记为正常、检查、隔离、感染或未知。
Protocol	会话使用的协议。
Public IP	分配给客户端的公共可路由 IP 地址。
Redirect URL	在安全状态验证或无客户端身份验证后，ACS将会话的访问策略下载到系统。Redirect URL 是访问策略负载的可选部分。系统将此远程主机的所有 HTTP（端口 80）和 HTTPS（端口 443）请求重定向至 Redirect URL（如果有）。如果访问策略不包含 Redirect URL， threat defense 设备不会重定向来自远程主机的 HTTP 和 HTTPS 请求。 重定向URL保持有效，直到IPsec会话结束或直到终端安全评估重新验证为止，对此，ACS 下载新的访问策略，其中可以包含其他重新定向 URL 或不包含重定向 URL。
Rekey Int (T or D)	IPsec（IKE）SA 加密密钥的生命期。T 值是持续时间，D 值是传输的数据。仅显示远程访问 VPN 的 T 值。
Rekey Left (T or D)	IPsec（IKE）SA加密密钥的剩余生命期。T值是持续时间，D值是传输的数据。仅显示远程访问 VPN 的 T 值。
Rekey Time Interval	IPsec（IKE）SA 加密密钥的生命期。
Remote IP addr	分配给隧道的远程终端（即远程对等设备上的接口）的 IP 地址。
Reval Int (T)	Revalidation Time Interval. 每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Reval Left (T)	到下次重新验证的时间。如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
重新验证时间间隔	每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Session ID	会话组件（子会话）的标识符。每个 SA 都有自己的标识符。
Session Type	会话的类型：LAN-to-LAN 或 Remote
SQ Int (T)	Status Query Time Interval. 每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是系统向远程主机发出的请求，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。

字段	Description
状态查询时间间隔	每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是系统向远程主机发出的请求，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。
Time Until Next Revalidation	如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
Tunnel Group	此隧道针对属性值引用的隧道组的名称。
UDP Dst Port or UDP Destination Port	远程对等设备用于 UDP 的端口号。
UDP Src Port or UDP Source Port	用于 UDP 的端口号。
Username	建立会话所使用的用户登录名称。
VLAN	分配给此会话的出口 VLAN 接口。系统将所有流量转发到此 VLAN。以下元素之一指定值：组策略或继承的组策略

示例

以下是 **show vpn-sessiondb** 命令的输出示例：

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ------------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
```

```
-------------------------------------------------------------------------------
Totals                        :      3 :         42
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
IPv6 Usage Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
-----------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
-------------------------------------------------------------------------------
```

以下是 **show vpn-sessiondb detail** 命令的输出示例：

```
> show vpn-sessiondb detail
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
-------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
-------------------------------------------------------------------------------
Totals                      :      3 :         42
-------------------------------------------------------------------------------
```

以下是 **show vpn-sessiondb detail l2l** 命令的输出示例：

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
```

```
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
Remote Addr : 209.165.201.30/255.255.255.0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel PFS Group : 5
Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 240 Bytes Rx : 160
Pkts Tx : 3 Pkts Rx : 2

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

以下是 **show vpn-sessiondb detail index 1** 命令的输出示例：

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
Session ID : 1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Aggressive Auth Mode : preSharedKeysXauth
Encryption : 3DES Hashing : MD5
```

```
Rekey Int (T): 86400 Seconds Rekey Left(T): 61078 Seconds
D/H Group : 2

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

NAC:
Reval Int (T): 3000 Seconds Reval Left(T): 286 Seconds
SQ Int (T) : 600 Seconds EoU Age (T) : 2714 Seconds
Hold Left (T): 0 Seconds Posture Token: Healthy
Redirect URL : www.cisco.com
```

以下是 **show vpn-sessiondb ospfv3** 命令的输出示例：

```
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

以下是 **show vpn-sessiondb detail ospfv3** 命令的输出示例：

```
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 105268 Seconds
Hold Left (T): 0 Seconds Posture Token:
```

```
Redirect URL :
```

以下是 **show vpn-sessiondb detail anyconnect** 命令的输出示例：

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab Index : 2
Assigned IP : 65.2.1.100 Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx : 0 Bytes Rx : 21248
Pkts Tx : 0 Pkts Rx : 238
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : test1
Login Time : 22:44:59 EST Tue Aug 13 2017
Duration : 0h:02m:42s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 75.2.1.60
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 400 Minutes Idle TO Left : 397 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : 3.1.05050

IKEv2:
Tunnel ID : 2.2
UDP Src Port : 64251 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86241 Seconds
PRF : SHA1 D/H Group : 2
Filter Name : mixed1
Client OS : Windows

IPsecOverNatT:
Tunnel ID : 2.3
Local Addr : 75.2.1.23/255.255.255.255/47/0
Remote Addr : 75.2.1.60/255.255.255.255/47/0
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport, GRE
Rekey Int (T): 28400 Seconds Rekey Left(T): 28241 Seconds
Idle Time Out: 400 Minutes Idle TO Left : 400 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Bytes Tx : 0 Bytes Rx : 21326
Pkts Tx : 0 Pkts Rx : 239
```

```
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 165 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

以下是 **show vpn-sessiondb ra-ikev2-ipsec** 命令的输出示例：

```
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 17844
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

以下是 **show vpn-sessiondb anyconnect** 命令的输出示例：

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                  Index        : 19576
Assigned IP  : 192.168.3.243          Public IP    : 192.168.10.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15060                  Bytes Rx     : 20631
Group Policy : DfltGrpPolicy          Tunnel Group : Ad_group
Login Time   : 09:24:53 UTC Fri Apr 7 2017
Duration     : 0h:03m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none                   Tunnel Zone  : 0
```

Related Commands

命令	Description
clear vpn-sessiondb statistics	清除 VPN 会话统计信息。

命令	Description
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。
show vpn-sessiondb summary	显示会话摘要，包括当前会话总数、每种类型的当前会话、峰值和累积总值、最大并发会话数。

show vpn-sessiondb ratio

要按协议或加密算法以百分比形式显示当前会话的比率，请使用 **show vpn-sessiondb ratio** 命令。

show vpn-sessiondb ratio {**encryption** | **protocol**} [**filter** *groupname*]

Syntax Description

encryption	显示使用每种加密方法的会话数和会话百分比。
protocol	显示使用每个 VPN 协议的会话数和会话百分比。
filter *groupname*	（可选。）过滤输出以仅包含所指定的隧道组的会话比率。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何根据加密显示会话比率。

```
> show vpn-sessiondb ratio encryption

Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Tunnels        Percent
none                     0                0%
DES                      0                0%
3DES                     0                0%
RC4                      0                0%
AES128                   4               80%
AES192                   1               20%
AES256                   0                0%
AES-GCM-128              0                0%
AES-GCM-192              0                0%
AES-GCM-256              0                0%
AES-GMAC-128             0                0%
AES-GMAC-192             0                0%
AES-GMAC-256             0                0%
```

以下示例显示如何根据协议显示会话比率。

```
> show vpn-sessiondb ratio protocol

Filter Group         : All
Total Active Tunnels : 3
Cumulative Tunnels   : 42

Protocol                 Tunnels        Percent
IKEv1                    0                0%
IKEv2                    0                0%
IPsec                    0                0%
```

```
IPsecLAN2LAN              0               0%
IPsecLAN2LANOverNatT      0               0%
IPsecOverNatT             0               0%
IPsecOverTCP              0               0%
IPsecOverUDP              0               0%
L2TPOverIPsec             0               0%
L2TPOverIPsecOverNatT     0               0%
Clientless                0               0%
Port-Forwarding           0               0%
IMAP4S                    0               0%
POP3S                     0               0%
SMTPS                     0               0%
AnyConnect-Parent         1              33%
SSL-Tunnel                1              33%
DTLS-Tunnel               1              33%
```

Related Commands

命令	Description
show vpn-sessiondb	显示有关 VPN 会话的信息。
show vpn-sessiondb summary	显示会话摘要，包括当前会话总数、每种类型的当前会话、峰值和累积总值、最大并发会话数。

show vpn-sessiondb summary

要显示活动会话数的摘要，请使用 **show vpn-sessiondb summary** 命令。

show vpn-sessiondb summary

Command History

版本	修改
6.1	引入了此命令。

使用指南

下表解释了活动会话和会话信息摘要中的字段：

字段	Description
Concurrent Limit	此系统上允许的并发活动会话的最大数量。
Cumulative Sessions	自上次启动或重置系统以来所有类型的会话数。
LAN-to-LAN	当前处于活动状态的 IPsec LAN-to-LAN 会话数。
Peak Concurrent	自上次启动或重置系统以来并发活动的所有类型会话的最大数量。
Percent Session Load	使用中的 VPN 会话分配的百分比。此值等于活动会话总数除以可用会话的最大数量（以百分比形式显示）。
Remote Access	ra-ikev1-ipsec - IKEv1 IPsec 远程访问用户数、L2TP over IPsec 以及通过当前活动的 NAT 会话的 IPsec。
Total Active Sessions	当前处于活动状态的所有类型会话的数量。

示例

以下是 **show vpn-sessiondb summary** 命令的输出示例：

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-----------------------------------------------
OSPFv3 IPsec : 1 : 1 : 1
-------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
-------------------------------------------------------------------------
```

以下是常规 IKEv2 IPsec 远程访问会话的 **show vpn-sessiondb summary** 命令的输出示例：

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
Generic IKEv2 Remote Access : 1 : 1 : 1
-------------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
----------------------------------------------
IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1
-------------------------------------------------------------------------------
Totals : 2 : 2
-------------------------------------------------------------------------------
```

Related Commands

命令	Description
show vpn-sessiondb	显示有关 VPN 会话的信息。
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。

show vrf

要显示有关系统上定义的虚拟路由器的信息，请使用 **show vrf** 命令。

show vrf ［**counters** | **lock**］

Syntax Description

counters	（可选）显示此系统上允许的用户定义的最大虚拟路由器数量，以及配置的实际虚拟路由器数量。最大计数文档不包括全局虚拟路由器：例如，如果最大计数为 4，则总数限制为 5。
lock	（可选）显示 VRF 锁定信息。

Command Default

如果不使用关键字， 命令会显示当前虚拟路由器以及分配给每个虚拟路由器的接口。

Command History

版本	修改
6.6	引入了此命令。

使用指南

如果启用了虚拟路由和转发 (VRF)，请使用 **show vrf** 命令查看有关系统上定义的虚拟路由器的基本信息。要查看每个虚拟路由器的路由表，请对 IPv4 路由表使用 。 **show route vrf** 名称 命令，对 IPv6 路由表使用 **show ipv6 route vrf** 名称 。

示例

以下示例显示了虚拟路由器和分配给每个路由器的接口：

```
> show vrf

Name            VRF ID          Description             Interfaces
vrf1            1                                       inside
                                                        inside_2
vrf2            2                                       inside_3
                                                        inside_4
```

以下示例显示了此系统上允许的最大虚拟路由器数量，以及当前虚拟路由器的数量。虚拟路由器是 IPv4、IPv6 还是两者兼有，取决于您为每个虚拟路由器内的接口分配的 IP 地址。请注意，最大数量是指用户定义的虚拟路由器；在本示例中，对于 VMware 系统，允许的总限制为 15，其中一个用于全局虚拟路由器，14 个用于用户定义的路由器。

```
> show vrf counters
Maximum number of VRFs supported: 14
Maximum number of IPv4 VRFs supported: 14
Maximum number of IPv6 VRFs supported: 14
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

以下示例显示 VRF 锁定信息。

```
> show vrf lock

VRF Name: single_vf; VRF id = 0 (0x0)
VRF lock count: 1
VRF Name: vrf1; VRF id = 1 (0x1)
VRF lock count: 2
VRF Name: vrf2; VRF id = 2 (0x2)
VRF lock count: 2
```

Related Commands

命令	Description
show ipv6 route	显示 IPv6 路由表。
show route	显示 IPv4 路由表。

show wccp

要显示与 Web 缓存通信协议 (WCCP) 相关的全局统计信息，请使用 **show wccp** 命令。

show wccp {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]
show wccp [**interfaces** [**detail**]]

Syntax Description

buckets	（可选）显示服务组存储桶分配。
detail	（可选）显示关于路由器和所有 Web 缓存的信息。
hash *dest_addr source_addr dest_port source_port*	（可选）显示指定连接的 WCCP 散列： • *dest_addr* 是目的主机的 IP 地址。 • *source_addr* 是源主机的 IP 地址。 • *Dest_port* 是目标主机的端口。 • *source_port* 是源主机的端口。
interfaces [**detail**]	（可选）显示 WCCP 重定向接口。包括用于接口配置的 detail 关键字。
service	（可选）显示服务组定义信息。
service-number	缓存所控制的 Web 缓存服务组的标识号。数字可以是 0 到 254。对于使用 Cisco Cache Engine 的 Web 缓存，以值 99 指示反向代理服务。
view	（可选）显示已检测或尚未检测特定服务组的其他成员。
web-cache	指定 Web 缓存服务的统计信息。

Command History

版本	修改
6.2	引入了此命令。

示例

以下示例展示如何显示 WCCP 信息：

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
```

```
Total Packets Redirected:           0
Redirect access-list:               foo
Total Connections Denied Redirect:  0
Total Packets Unassigned:           0
Group access-list:                  foobar
Total Messages Denied to Group:     0
Total Authentication failures:      0
Total Bypassed Packets Received:    0
```

Related Commands

命令	Description
clear wccp	清除统计数据。

show webvpn

要查看有关远程接入 VPN 的信息，请使用 **show webvpn** 命令。

show webvpn {**anyconnect** | **debug-condition** | **group-alias** [*tunnel_group*] | **group-url** [*tunnel_group*] | **statistics**}

Syntax Description

anyconnect	显示有关可下载到客户端终端的 AnyConnect 映像的信息。
debug-condition	显示 **debug webvpn condition** 命令设置的当前调试条件。
group-alias [*tunnel_group*]	显示隧道组的别名（连接配置文件）。您可以选择指定隧道组的名称，以仅查看有关该组的信息。每个组可以有多个别名或甚至没有别名。
group-url [*tunnel_group*]	显示隧道组（连接配置文件）的 URL。您可以选择指定隧道组的名称，以仅查看有关该组的信息。每个组可以有多个 URL 或甚至没有 URL。
statistics	显示有关 WebVPN 事件的数据。

Command History

版本	修改
6.2.1	引入了此命令。
7.1	有关外部浏览器软件包的信息已添加到 AnyConnect 输出中。

示例

以下示例显示 **show webvpn anyconnect** 命令的输出示例：

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
  CISCO STC win2k+
  4,2,06014
  Hostscan Version 4.2.06014
  Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

以下 **show webvpn anyconnect** 示例包括外部浏览器软件包（如果与 SAML 身份验证配合使用）。

```
> show webvpn anyconnect
1. disk0:/anyconnpkgs/anyconnect-win-4.10.01075-webdeploy-k9.pkg 2 dyn-regex=/Windows NT/
  CISCO STC win2k+
  4,10,01075
  Hostscan Version 4.10.01075
  Wed 04/28/2021 12:36:03.98

1 AnyConnect Client(s) installed
```

```
2. disk0:/externalbrowserpkgs/external-sso-98.161.00015-webdeploy-k9.pkg
  Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 05/05/21 15:49:27.817381
```

以下示例显示 **show webvpn debug-condition** 命令的输出示例：

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

以下示例显示 **show webvpn group-alias** 命令的输出示例：

```
> show webvpn group-alias
Tunnel Group: Ad_group   Group Alias: ad_group enabled
Tunnel Group: Radius_group   Group Alias: Radius_group enabled
Tunnel Group: Cert_auth   Group Alias: cert_auth enabled
```

以下示例显示 **show webvpn group-url** 命令的输出示例：

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

以下示例显示 **show webvpn statistics** 命令的输出示例：

```
> show webvpn statistics
Total number of objects served  0
 html                           0
 js                             0
 css                            0
 vb                             0
 java archive                   0
 java class                     0
 image                          0
 undetermined                   0
Server compression statistics
 Decompression success from server                  0
 Unsolicited compression from server                0
 Unsupported compression algorithm used by server   0
 Decompression failure for server responses         0
IOBuf failure statistics
 uib_create_with_channel                            0
 uib_create_with_string                             0
 uib_create_with_string_and_channel                 0
 uib_transfer                                       0
 uib_add_filter                                     0
 uib_yyread                                         0
 uib_read                                           0
 uib_set_buffer_max                                 0
 uib_set_eof_symbol                                 0
 uib_get_capture_handle                             0
 uib_set_capture_handle                             0
 uib_buflen                                         0
 uib_bufptr                                         0
```

```
uib_buf_endptr                          0
uib_get_buf_offset                      0
uib_get_buf_offset_addr                 0
uib_get_nth_char                        0
uib_consume                             0
uib_advance_bufptr                      0
uib_eof                                 0
```

show xlate

要显示有关 NAT 会话（转换或转换）的信息，请使用 **show xlate** 命令。

show xlate ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］
show xlate count

Syntax Description

count	显示转换计数。
global *ip1*[*-ip2*]	（可选）按映射 IP 地址或地址范围显示活动的转换。
gport *port1*[*-port2*]	按映射端口或端口范围显示活动的转换。
interface *if_name*	（可选）按接口显示活动转换。
local *ip1*[*-ip2*]	（可选）按实际 IP 地址或地址范围显示活动的转换。
lport *port1*[*-port2*]	按实际端口或端口范围显示活动的转换。
netmask *mask*	（可选）指定用于限定映射的或实际 IP 地址的网络掩码。
type *type*	（可选）按类型显示活动的转换。您可以输入以下一个或多个类型： • **static** • **portmap** • **dynamic** • **twice-nat** （也称为手动 NAT） 指定多个类型时，请用空格来分隔类型。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show xlate 命令显示转换槽的内容。转换可以包括为内部接口生成的转换，这些转换不会显示在设备管理器的 NAT 规则表中。这些是内部处理所必需的。

当 VPN 客户端配置已启用且内部主机发出 DNS 请求时， **show xlate** 命令可以为静态转换列出多个 xlate。

在集群环境中，可将最多三个 xlate 复制到集群中的不同节点以处理 PAT 会话。在拥有该连接的设备上创建了一个 xlate。在其他设备上创建一个 xlate 以备份 PAT 地址。最后，导向器上存在一个可复制该流的 xlate。在备用和导向器是同一设备的情况下，可能创建两个（而不是三个）xlate。

示例

以下是 **show xlate** 命令的输出示例。nlp_int_tap 的初始 PAT 转换与允许 设备管理器 访问 192.168.1.1 而非管理接口地址的 HTTPS 访问规则相关。这些是内部 NAT 转换，其规则不会显示在设备管理器的 NAT 表中。

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

以下是来自 **show xlate** 命令的输出示例，其中显示从 IPv4 到 IPv6 的转换

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

Related Commands

命令	Description
clear xlate	清除当前转换和连接信息。
show conn	显示所有活动连接。
show local-host	显示本地主机网络信息。

show zone

要显示流量区域信息，请使用 **show zone** 命令。

show zone ［*name*］

Syntax Description

name	（可选）流量区域的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

流量区域与安全区域不完全相同。虽然被动安全区域也会自动生成为流量区域，但路由和交换安全区域不会自动生成。流量区域用以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的不对称路由。

要查看区域配置的其余部分，请使用 **show running-config zone** 和 **show running-config interface** 命令。

示例

以下示例显示已配置的流量区域。在本示例中，流量区域用于被动接口。如果区域用于等价多路径路由，则区域类型将为 ecmp。接口配置如下。 **zone-member** 命令将接口配置为区域的成员。

```
> show zone passive-security-zone
Zone: passive-security-zone passive
    Security-level: 0
    Zone member(s): 1
      passive                       GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 mode passive
 nameif passive
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 zone-member krjones-passive-security-zone
```

Related Commands

命令	Description
clear conn zone	清除区域连接。
clear local-host zone	清除区域主机。
show interface	显示接口的运行时间状态和统计信息。

命令	Description
show local-host zone	显示区域内本地主机的网络状态。
show nameif zone	显示接口的区域或内联集成员身份。

shun

要阻止来自攻击主机的连接，请使用 **shun** 命令。要禁用 shun，请使用此命令的 **no** 形式。

shun *source_ip* ［*dest_ip source_port dest_port* ［*protocol*］］［**vlan** *vlan_id*］
no shun *source_ip* ［**vlan** *vlan_id*］

Syntax Description

dest_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标端口。
dest_ip	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标地址。
protocol	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的 IP 协议，例如 UDP 或 TCP。默认情况下，protocol 为 0（任何协议）。
source_ip	指定攻击主机的地址。如果仅指定源 IP 地址，则以后来自此地址的所有连接都将被丢弃；当前连接保持不变。要丢弃当前连接并同时放置 shun，请指定连接的其他参数。请注意，shun 适用于后面所有来自源 IP 地址的连接，无论目标参数为何。
source_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的源端口。
vlan *vlan_id*	（可选）指定源主机所在的 VLAN ID。

Command Default

默认协议是 0（任何协议）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

shun 命令可以阻止来自攻击主机的连接。后面来自源 IP 地址的所有连接都将被丢弃并记录，直到手动取消阻止功能。无论使用指定主机地址的连接当前是否为活动状态， **shun** 命令的阻止功能都适用。

如果您指定目标地址、来源和目标端口以及协议，则会丢弃匹配的连接以及在后面所有来自源 IP 地址的连接上放置 shun；将会避开后面所有的连接，而不只是与这些特定连接参数匹配的连接。

对每个源 IP 地址只能使用一个 **shun** 命令。

由于 **shun** 命令用于动态阻止攻击，因此不会显示在 threat defense 设备配置中。

只要删除接口配置，所有附加到该接口的 shun 也会一同删除。

示例

以下示例展示攻击主机 (10.1.1.27) 使用 TCP 与受攻击主机 (10.2.2.89) 建立连接。 threat defense 设备连接表中的连接如下所示：

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

使用以下选项应用 **shun** 命令：

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

此命令将从 threat defense 设备连接表删除特定的当前接通，同时禁止来自 10.1.1.27 的所有后续数据包通过 threat defense 设备。

Related Commands

命令	Description
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
show conn	显示所有活动连接。
show shun	显示 shun 信息。

shutdown

要关闭设备，请使用 **shutdown** 命令。

shutdown

Command History

版本	修改
6.0.1	引入了此命令。

示例

以下示例是关闭设备时 **shutdown** 命令的输出示例：

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

Related Commands

命令	Description
reboot	重启设备。

system access-control clear-rule-counts

要将访问控制规则命中次数重置为 0，请使用 **system access-control clear-rule-counts** 命令。

system access-control clear-rule-counts

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 **system access-control clear-rule-counts** 命令的输出示例：

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

Related Commands

命令	Description
show access-control-config	显示访问控制策略摘要和命中计数。

system generate-troubleshoot

要在思科技术支持部门要求时生成故障排除数据以供分析，请使用 **system generate troubleshoot** 命令。

system generate-troubleshoot 选项

Syntax Description

选项	显示要生成的故障排除数据的类型。您可以输入一个或多个选项。使用空格隔开多个选项。 • **ALL**-运行以下所有选项。 • **SNT**-Snort 性能和配置。 • **PER**-硬件性能和日志。- • **SYS**-系统配置、策略和日志。 • **DES**-检测配置、策略和日志。 • **NET**-接口和网络相关数据。 • **VDB**-发现、感知、VDB 数据和日志。 • **UPG**-升级数据和日志。 • **DBO**-所有数据库数据。 • **LOG**-所有日志数据。 • **NMP**-网络映射信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何为 Snort 和硬件性能生成故障排除数据。

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

Related Commands

命令	Description
copy	从系统复制文件或将文件复制到系统。
delete	从系统中删除文件。

system lockdown-sensor

要删除对专家模式和 Bash Shell 的访问，请使用 **system lockdown-sensor** 命令。

system lockdown-sensor

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

注意 不能撤销此命令。如果您需要恢复对专家模式的访问，您必须联系思科技术支持中心并获取热补丁。

expert 命令提供对 Bash shell 的访问，为管理用户提供对系统操作环境的广泛访问。安全认证机制（例如通用标准 (CC) 或统一功能批准产品列表 (UC APL)）强加了限制系统用户可用的访问权限和信息的要求。使用 **system lockdown-sensor** 命令可删除对 **expert** 命令的访问，以帮助满足这些认证要求。

注释 使用此命令后， **expert** 命令在当前 SSH 会话中仍然可用。您必须注销并重新登录，以验证该命令是否已删除且不再有效。在您使用 命令后登录的任何其他人也将无法使用专家模式。

示例

以下示例删除对专家模式的访问，以满足安全要求。

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
>
```

system support commands

大多数系统支持命令用于在思科技术支持中心的帮助下进行调试和故障排除。您应在思科支持人员的指导下使用这些命令，但以下命令除外，这些命令是通用的。

- system support diagnostic-cli， 第 121 页
- system support view-files， 第 126 页
- system support ssl-hw- commands， 第 123 页

system support ssl-client-hello- commands

这些命令允许您确定传输层安全 (TLS) 1.3 降级到 TLS 1.2 的行为。由于受管设备不支持 TLS 1.3 加密或解密，因此客户端和服务器之间的 TLS 1.3 会话可能会中断，从而导致客户端网络浏览器中出现如下错误：

ERR_SSL_PROTOCOL_ERROR

SEC_ERROR_BAD_SIGNATURE

ERR_SSL_VERSION_INTERFERENCE

当客户端连接到服务器并且 TLS 检查确定已修改为降级的连接与 **不解密** SSL 规则操作匹配时，可能会发生错误。

我们建议您在咨询思科 TAC 之后再使用这些命令。

system support ssl-client-hello-enabled aggressive_tls13_downgrade { **true** | **false** }

Syntax Description

true	默认值。每当需要执行解密时，TLS 1.3 连接都会降级。但是，如果在 ClientHello 消息之后收到的数据导致会话匹配 **不解密** 规则，则会话可能会失败。
false	仅当合理确定会话与 **不解密** 规则不匹配时，才会降级 TLS 1.3 连接。在某些情况下，需要解密的 TLS 连接可能不会降级。在这些情况下，流量不会被解密。改为执行 SSL 策略中 **无法解密的操作** 的 **会话未缓存** 设置指定的操作。

Command History

版本	修改
6.2.3.7	引入了此命令。

system support diagnostic-cli

要进入诊断 CLI（包括其他 show 和其他故障排除命令），请使用 **system support diagnostic-cli** 命令。

system support diagnostic-cli

Command History

版本	修改
6.1	引入了此命令。

使用指南

诊断 CLI 包含可用于对系统进行故障排除的其他 show 和其他命令。诊断 CLI 中的命令来自 ASA 软件。常规 threat defense CLI 包含许多相同的命令，因此您可能不需要诊断 CLI 的额外命令。

当您进入诊断 CLI 时，您将处于与常规 threat defense CLI 不同的会话中。

提示符会更改为包括系统主机名。有两种模式，提示符指示您所处的模式。对于用户 EXEC 模式，提示符为：

```
hostname>
```

对于特权 EXEC 模式（也称为启用模式），提示符如下。使用 enable 命令进入此模式。虽然系统会提示您输入密码，但只需按 Enter 键即可，默认情况下无需密码即可进入此模式。

```
hostname#
```

使用诊断 CLI 时，请记住以下提示：

- 要退出诊断 CLI 并返回到常规 CLI，请按 Ctrl+a，然后按 d。
- 使用 **exit** 命令以退出特权 EXEC 模式。

  每种模式下可用的命令各不相同。特权 EXEC 模式包含的命令明显多于用户 EXEC 模式。使用 **?** 查看可用的命令。您可以在 ASA 软件命令参考中找到使用信息：

  - 思科 ASA 系列命令参考，A - H 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html
  - 思科 ASA 系列命令参考，I - R 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html
  - 思科 ASA 系列命令参考，S 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - 思科 ASA 系列命令参考，ASASM 的 T-Z 命令和 IOS 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- 诊断 CLI 可以包含对 threat defense无意义的命令。如果您尝试不提供有意义（或任何）信息的命令，则 threat defense可能未配置或不支持相关功能。

- 诊断 CLI 不允许您进入配置模式。您无法使用 CLI 配置设备。
- 当您从诊断 CLI 中分离时，下次进入时，您将处于与上次分离时相同的模式。
- 在 ASA 5506W-X 上，您可以使用 **session wlan** 命令打开与无线模块的连接，并使用其 CLI 配置无线接入点。必须在特权 EXEC 模式下。

示例

以下示例显示如何进入诊断 CLI 和特权 EXEC 模式。输入 **enable** 命令后出现密码提示时，只需按 Enter 键即可。默认情况下，没有进入特权 EXEC 模式的密码。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

system support ssl-hw- commands

这些命令允许您对版本 6.2.3 和 6.3 中称为 *TLS/SSL* 硬件加速，以及版本 6.4 中称为 *TLS* 加密加速 的功能执行各种操作。可用的关键字取决于 threat defense 软件版本。

支持的设备以及默认情况下是启用还是禁用功能还取决于软件版本。有关详细信息，请参阅 管理中心 配置指南。

版本 6.2.3 和 6.3 的语法：

system support {**ssl-hw-status** | **ssl-hw-supported-ciphers** | **ssl-hw-offload enable** | **ssl-hw-offload disable**}

版本 6.4 的语法：

system support ssl-hw-supported-ciphers

Syntax Description

ssl-hw-status	显示 SSL 硬件加速的当前状态。默认状态为： • 6.2.3：禁用 • 6.3 和 6.4：已启用
ssl-hw-supported-ciphers	显示 SSL 硬件加速支持的密码列表。此命令非常有用，因为 SSL 硬件加速不支持 SSL 软件加速支持的所有密码（特别是不支持解密 SEED 和 Camellia 密码）。
ssl-hw-offload enable	启用 SSL 硬件加速；系统将提示您重新启动设备。
ssl-hw-offload disable	禁用 SSL 硬件加速；系统将提示您重新启动设备。

Command History

版本	修改
6.4	功能名称由 TLS/SSL 硬件加速 更改为 TLS 加密加速。 已删除以下关键字： **ssl-hw-offload enable** **ssl-hw-offload disable** **ssl-hw-status**
6.3	默认情况下启用此功能。
6.2.3	引入了此命令。默认情况下会禁用此功能。

使用指南

注释 在本节讨论的命令中， **system support ssl-hw-offload-supported ciphers** 仅适用于版本 6.4。

使用这些命令可显示有关 SSL 硬件加速 的信息，或者启用或禁用该功能。

启用 SSL 硬件加速以提高加密和解密性能。

禁用 SSL 硬件加速以使用其不支持的任何功能，或者在启用 SSL 策略的情况下遇到意外流量中断。

SSL 硬件加速不支持的功能包括：

- 启用了 威胁防御 容器实例 的托管设备。
- 如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

  此行为受 **configure snort preserve-connection {enable | disable}** 命令控制。

使用 **system support ssl-hw-status** 命令显示当前状态。

使用 **system support ssl-hw-supported-ciphers** 命令显示 SSL 硬件加速支持的密码列表。

示例

以下是查看 SSL 硬件加速的当前状态的示例：

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

以下是启用 SSL 硬件加速并提示重启设备的示例：

```
If you enable SSL hardware acceleration, you cannot:
    1.    Decrypt passive or inline tap traffic.
    2.    Preserve Do Not Decrypt connections when the inspection engine restarts.
Continue? (y/n) [n]: y


Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]: y

SSL hardware acceleration will be enabled on system boot.
```

在重新启动设备之前，您需要确认所有上述内容。

以下是 SSL 硬件加速支持的部分密码列表：

```
> system support ssl-hw-supported-ciphers
CID     Cipher Suite Name                                CH_mod Keep     Support Inline
Support Passive
-------------------------------------------------------------------------------------------------
0x0004  TLS_RSA_WITH_RC4_128_MD5                         Yes             Yes             Yes
0x0005  TLS_RSA_WITH_RC4_128_SHA                         Yes             Yes             Yes
0x0009  TLS_RSA_WITH_DES_CBC_SHA                         Yes             Yes             Yes
```

```
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA                Yes             Yes             Yes
0x000c  TLS_DH_DSS_WITH_DES_CBC_SHA                  No              No              No
0x000d  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA             No              No              No
0x000f  TLS_DH_RSA_WITH_DES_CBC_SHA                  No              No              No
0x0010  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA             No              No              No
0x0012  TLS_DHE_DSS_WITH_DES_CBC_SHA                 No              No              No
0x0013  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA            No              No              No
0x0015  TLS_DHE_RSA_WITH_DES_CBC_SHA                 Yes             Yes             No
0x0016  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA            Yes             Yes             No
0x0018  TLS_DH_Anon_WITH_RC4_128_MD5                 No              Yes             No
0x001a  TLS_DH_Anon_WITH_DES_CBC_SHA                 No              Yes             No
0x001b  TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA            No              Yes             No
0x001e  TLS_KRB5_WITH_DES_CBC_SHA                    No              No              No
0x001f  TLS_KRB5_WITH_3DES_EDE_CBC_SHA               No              No              No
0x0020  TLS_KRB5_WITH_RC4_128_SHA                    No              No              No
0x0024  TLS_KRB5_WITH_RC4_128_MD5                    No              No              No
0x002f  TLS_RSA_WITH_AES_128_CBC_SHA                 Yes             Yes             Yes
0x0030  TLS_DH_DSS_WITH_AES_128_CBC_SHA              No              No              No
0x0031  TLS_DH_RSA_WITH_AES_128_CBC_SHA              No              No              No
... more
```

system support view-files

要在与思科技术支持中心 (TAC) 合作解决问题时查看系统日志内容，请使用 **system support view-files** 命令。

system support view-files

Command History

版本	修改
6.1	引入了此命令。

使用指南

system support view-files 命令可打开系统日志。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

该命令将显示一个菜单供您选择日志。请使用以下命令在向导中导航：

- 要更改为子目录，请键入该目录的名称并按 Enter 键。
- 要选择欲查看的文件，请在提示符后输入 **s**。然后系统将提示您输入文件名。请键入完整名称，并注意区分大小写。文件列表会显示日志的大小，您最好考虑一下再打开非常大的日志。
- 看到 --More-- 时，按空格键可查看下一页日志条目；按 Enter 键仅查看下一个日志条目。到达日志末尾后，即会转到主菜单。--More-- 行会显示日志的大小和已查看部分的大小。**如果不想翻阅完整个日志，请使用 Ctrl+C 关闭日志并退出命令**。
- 键入 **b** 返回菜单结构的上一级。

如果要保持日志打开以便及时看到添加的新消息，请使用 **tail-logs** 命令而非 。

示例

以下示例显示如何查看 ngfw.log 文件。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
```

```
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

Related Commands

命令	Description
tail-logs	打开日志并保持打开状态。

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。