show p - show r

show packet tracer

要显示有关 pcap trace 输出的信息，请使用 **show packet tracer** 命令。

show packet-tracer pcap trace ［ **packet-number** *number* | **summary** | **detailed** | **status** ］

Syntax Description

packet-number	（可选）显示 pcap 中单个数据包的跟踪输出。
summary	（可选）显示 pcap 摘要。
detailed	（可选）显示 pcap 中所有数据包的跟踪输出。
status	（可选）显示 pcap trace 的当前执行状态。

Command Default

无默认行为或值。

Command History

版本	修改
7.1	该命令已增强，包括 pcap trace 的输出。

使用指南

show packet-tracer 命令显示数据包跟踪器输出。 **pcap trace** 命令允许您显示最近在 PCAP 文件上运行的 packet-tracer 的跟踪缓冲区输出。

示例

以下是 **show packet-tracer pcap trace summary** 命令的输出示例：

```
> show packet-tracer pcap trace summary
      1: 02:38:01.265123       6.1.1.100.51944 > 9.1.1.100.80: S 542888804:542888804(0) win
 29200 <mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7>
      2: 02:38:01.271317       9.1.1.100.80 > 6.1.1.100.51944: S 2281169942:2281169942(0)
ack 542888805 win 28960 <mss 1380,sackOK,timestamp 2526520070 2526545680,nop,wscale 7>
      3: 02:38:01.271638       6.1.1.100.51944 > 9.1.1.100.80: . ack 2281169943 win 229
<nop,nop,timestamp 2526545682 2526520070>

               Total packets: 3
       Packets replayed: 3
       Result: Allow
       Start time: Mar 28 04:51:54
       Total time taken: 10247935ns
     show packet-tracer pcap trace packet-number 1 detailed
     1: 02:38:01.265123 0050.56a9.81e5 0050.56a9.60e1 0x0800 Length: 74
      6.1.1.100.51944 > 9.1.1.100.80: S [tcp sum ok] 542888804:542888804(0) win 29200 <mss
 1460,sackOK,timestamp 2526545680 0,nop,wscale 7> (DF) (ttl 64, id 54388)
      Phase: 1
      Type: ACCESS-LIST
      Subtype:
      Result: ALLOW
      Time Spent: 12345 ns
      Config:
      Implicit Rule
      Additional Information:
```

```
Forward Flow based lookup yields rule:
 in  id=0x154523db3ce0, priority=1, domain=permit, deny=false
                hits=92, user_data=0x0, cs_id=0x0, l3_type=0x8
                src mac=0000.0000.0000, mask=0000.0000.0000
                dst mac=0000.0000.0000, mask=0100.0000.0000
                input_ifc=inside, output_ifc=any
 ...
 ...
```

Related Commands

命令	Description
packet tracer	根据防火墙的当前配置生成 5 到 6 元组数据包

show packet-statistics

要显示 Secure Firewall 3100上有关非策略相关数据包丢弃的信息，请使用 **show packet-statistics** 命令。在 威胁防御上，在系统诊断模式下运行此命令。

show packet-statistics { **interface id** *slot port* } [**breakout** *port* | { **brief** | **no brief** }]

Syntax Description

interface id*slotport*	显示统计信息的带有插槽号和端口号的接口名称。
breakout	（可选）以太网端口号的分支。
brief	（可选）显示不包括零计数器值的输出。

Command Default

无默认行为或值。

Command History

版本	修改
7.2	引入了此命令。

使用指南

show packet-statistics 命令会整理并显示来自多个来源的丢包数据。输出有助于确定数据包被丢弃的位置。此命令整合了以下调试命令的输出：

- **show portmanager counters ethernet <slot> <port>**
- **show queuing interface ethernet <slot> <port>**
- **show portmanager counters internal <slot> <port>**
- **show queuing interface internal <slot> <port>**
- **show portmanager switch counters packet-trace**
- **show npu-accel statistics**
- **show interface detail**
- **show asp drop**

当流量到达设备时，合并的输出按数据路径的顺序排列。此外，输出不会被其他 CLI 的输出中断或中断。

slot/port and **breakout***port* 用于限制特定接口的输出。这些变量和关键字仅适用于外部交换机端口和 Lina 接口。对于其他接口，这些变量将被忽略。

示例

以下是 **show packet-statistics** 命令的输出示例：

```
$ show packet-statistics ethernet 2/1/1 no brief

====================== show portmanager switch counters packet-trace ======================


       Counter                              Description
---------------------- ------------------------------------------------------
goodOctetsRcv          Number of ethernet frames received that are not bad
                       ethernet frames or MAC Control pkts
badOctetsRcv           Sum of lengths of all bad ethernet frames received
gtBrgInFrames          Number of packets received
gtBrgVlanIngFilterDisc Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc     Number of packets discarded due to
                       Security Filtering measures
gtBrgLocalPropDisc     Number of packets discarded due to reasons other than
                       VLAN ingress and Security filtering
dropCounter            Ingress Drop Counter
outUcFrames            Number of unicast packets transmitted
outMcFrames            Number of multicast packets transmitted. This includes
                       registered multicasts, unregistered multicasts
                       and unknown unicast packets
outBcFrames            Number of broadcast packets transmitted
brgEgrFilterDisc       Number of IN packets that were Bridge Egress filtered
txqFilterDisc          Number of IN packets that were filtered
                       due to TxQ congestion
outCtrlFrames          Number of out control packets
                       (to cpu, from cpu and to  analyzer)
egrFrwDropFrames       Number of packets dropped due to egress
                       forwarding restrictions
goodOctetsSent         Sum of lengths of all good ethernet
                       frames sent from this MAC


        Counter            Source port- 0/0    Destination port- 0/0
-----------------------  ---------------------  ---------------------
goodOctetsRcv                    ---                    ---
badOctetsRcv                      ---                    ---

                                      Ingress counters
gtBrgInFrames                   9515                   9515
gtBrgVlanIngFilterDisc             0                      0
gtBrgSecFilterDisc                 0                      0
gtBrgLocalPropDisc                 0                      0
dropCounter                      319           Only for source-port

                                      Egress counters
outUcFrames                       12                     12
outMcFrames                     8176                   8176
outBcFrames                     1008                   1008
brgEgrFilterDisc                   0                      0
txqFilterDisc                      0                      0
outCtrlFrames                      0                      0
egrFrwDropFrames                   0                      0

goodOctetsSent                    ---                    ---

Error at clearing mac counters0/0: GT_BAD_PARAM = Illegal parameter in function called


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

====================== show npu-accel statistics ======================
module: kc25-pcie, pipe: 0
```

```
--------------------------
reg_pcie_rcv_reg_access_rd_tlp_cnt = 28374275
reg_pcie_rcv_reg_access_wr_tlp_cnt = 3810207

module: kc25-eth, pipe: 0
-------------------------
stat_rx_bip_err_0 = 0
stat_rx_bip_err_1 = 0
stat_rx_bip_err_2 = 0
stat_rx_bip_err_3 = 0
stat_rx_framing_err_0 = 0
stat_rx_framing_err_1 = 0
stat_rx_framing_err_2 = 0
stat_rx_framing_err_3 = 0
stat_rx_bad_code = 0
stat_tx_frame_error = 0
stat_tx_total_packets = 0
stat_tx_total_good_packets = 0
stat_tx_total_bytes = 0
stat_tx_total_good_bytes = 0
stat_tx_packet_64_bytes = 0
stat_tx_packet_65_127_bytes = 0
stat_tx_packet_128_255_bytes = 0
stat_tx_packet_256_511_bytes = 0
stat_tx_packet_512_1023_bytes = 0
stat_tx_packet_1024_1518_bytes = 0
stat_tx_packet_1519_1522_bytes = 0
stat_tx_packet_1523_1548_bytes = 0
stat_tx_packet_1549_2047_bytes = 0
stat_tx_packet_2048_4095_bytes = 0
stat_tx_packet_4096_8191_bytes = 0
stat_tx_packet_8192_9215_bytes = 0
stat_tx_packet_large = 0
stat_tx_packet_small = 0
stat_tx_bad_fcs = 0
stat_tx_unicast = 0
stat_tx_multicast = 0
stat_tx_broadcast = 0
stat_tx_vlan = 0
stat_tx_pause = 0
stat_tx_user_pause = 0
stat_rx_total_packets = 964
stat_rx_total_good_packets = 964
stat_rx_total_bytes = 264439
stat_rx_total_good_bytes = 264439
stat_rx_packet_64_bytes = 0
stat_rx_packet_65_127_bytes = 35
stat_rx_packet_128_255_bytes = 0
stat_rx_packet_256_511_bytes = 929
stat_rx_packet_512_1023_bytes = 0
stat_rx_packet_1024_1518_bytes = 0
stat_rx_packet_1519_1522_bytes = 0
stat_rx_packet_1523_1548_bytes = 0
stat_rx_packet_1549_2047_bytes = 0
stat_rx_packet_2048_4095_bytes = 0
stat_rx_packet_4096_8191_bytes = 0
stat_rx_packet_8192_9215_bytes = 0
stat_rx_packet_large = 0
stat_rx_undersize = 0
stat_rx_fragment = 0
stat_rx_oversize = 0
stat_rx_toolong = 0
stat_rx_jabber = 0
stat_rx_bad_fcs = 0
```

```
stat_rx_packet_bad_fcs = 0
stat_rx_stomped_fcs = 0
stat_rx_unicast = 0
stat_rx_multicast = 0
stat_rx_broadcast = 964
stat_rx_vlan = 0
stat_rx_pause = 0
stat_rx_user_pause = 0
stat_rx_inrangeerr = 0
stat_rx_truncated = 0
eth_tx_good_pkt_cnt = 0
eth_tx_err_pkt_cnt = 0
eth_rx_good_pkt_cnt = 964
eth_tx_fifo_sbit_err_cnt = 0
eth_tx_fifo_dbit_err_cnt = 0
eth_rx_fifo_sbit_err_cnt = 0
eth_rx_fifo_dbit_err_cnt = 0

module: kc25-nic, pipe: 0
-------------------------
nic_top_in_pkt_cnt = 964
nic_top_tm_out_pkt_cnt = 971
nic_top_inband_flow_tbl_pkt_cnt = 7
nic_top_inband_stat_pkt_cnt = 0
tm_shared_mem_sbiterr_pkt_cnt = 0
tm_shared_mem_dbiterr_pkt_cnt = 0
tm_pkt_buf_sbiterr_pkt_cnt = 0
tm_pkt_buf_dbiterr_pkt_cnt = 0
tm_out_fifo_sbiterr_pkt_cnt = 0
tm_out_fifo_dbiterr_pkt_cnt = 0
tm_qm_mem_parerr_pkt_cnt = 0
tm_budm_mem_parerr_pkt_cnt = 0
tm_qm_taildrop_pkt_cnt = 0
tm_h2c_desc_mem_sbiterr_pkt_cnt = 0
tm_h2c_desc_mem_dbiterr_pkt_cnt = 0
tm_c2h_desc_mem_sbiterr_pkt_cnt = 0
tm_c2h_desc_mem_dbiterr_pkt_cnt = 0
tm_inband_fifo_sbiterr_pkt_cnt = 0
tm_inband_fifo_dbiterr_pkt_cnt = 0
tm_egr_fifo_sbiterr_pkt_cnt = 0
tm_egr_fifo_dbiterr_pkt_cnt = 0

Traffic Manager per Q statistics
qid             input pkts           output pkts   input tail-drop cnt
  0                     49                    49                     0
  1                      0                     0                     0
  2                     66                    66                     0
  3                      0                     0                     0
  4                     42                    42                     0
  5                      0                     0                     0
  6                     64                    64                     0
  7                      0                     0                     0
  8                      0                     0                     0
  9                     42                    42                     0
 10                      0                     0                     0
 11                     64                    64                     0
 12                      0                     0                     0
 13                     64                    64                     0
 14                      0                     0                     0
 15                     64                    64                     0
 16                      0                     0                     0
 17                     88                    88                     0
 18                      0                     0                     0
 19                     24                    24                     0
```

```
 20                      0                       0                       0
 21                     64                      64                       0
 22                     40                      40                       0
 23                     64                      64                       0
 24                     42                      42                       0
 25                     42                      42                       0
 26                     42                      42                       0
 27                      0                       0                       0
 28                      0                       0                       0
 29                     39                      39                       0
 30                     64                      64                       0
 31                      0                       0                       0
 32                      0                       0                       0
 33                      0                       0                       0
 34                      0                       0                       0
 35                      0                       0                       0
 36                      0                       0                       0
 37                      0                       0                       0
 38                      0                       0                       0
 39                      0                       0                       0
 40                      0                       0                       0
 41                      0                       0                       0
 42                      0                       0                       0
 43                      0                       0                       0
 44                      0                       0                       0
 45                      0                       0                       0
 46                      0                       0                       0
 47                      0                       0                       0
 48                      0                       0                       0
 49                      0                       0                       0
 50                      0                       0                       0
 51                      0                       0                       0
 52                      0                       0                       0
 53                      0                       0                       0
 54                      0                       0                       0
 55                      0                       0                       0
 56                      0                       0                       0
 57                      0                       0                       0
 58                      0                       0                       0
 59                      0                       0                       0
 60                      0                       0                       0
 61                      0                       0                       0
 62                      0                       0                       0
 63                      0                       0                       0

module: kc25-ingress-pkt-classifier, pipe: 0
---------------------------------------------
cla_opt_tbl_hit_cmd_cnt = 0
cla_opt_tbl_miss_cmd_cnt = 958
cla_tunnel_tbl_hit_cmd_cnt = 0
cla_tunnel_tbl_miss_cmd_cnt = 0
cla_6_tuple_tbl_hit_cmd_cnt = 0
cla_6_tuple_tbl_miss_cmd_cnt = 0
cla_4_tuple_tbl_hit_cmd_cnt = 0
cla_4_tuple_tbl_miss_cmd_cnt = 0
cla_bypass_in_cmd_cnt = 6
cla_non_bypass_in_cmd_cnt = 958
cla_rss_lookup_cmd_cnt = 958
cla_rss_bypass_cmd_cnt = 6
cla_opt_tbl_sbiterr_pkt_cnt = 0
cla_opt_tbl_dbiterr_pkt_cnt = 0
cla_tunnel_tbl_sbiterr_pkt_cnt = 0
cla_tunnel_tbl_dbiterr_pkt_cnt = 0
cla_6_tuple_tbl_sbiterr_pkt_cnt = 0
```

```
cla_6_tuple_tbl_dbiterr_pkt_cnt = 0
cla_4_tuple_tbl_sbiterr_pkt_cnt = 0
cla_4_tuple_tbl_dbiterr_pkt_cnt = 0
cla_vf_dma_qid_ram_dbiterr_pkt_cnt = 0
inbf_ram_sbiterr_cnt = 0
inbf_ram_dbiterr_cnt = 0
inbf_rx_request_pkt_cnt = 270327
inbf_tx_response_pkt_cnt = 7
inbf_parser_regrd_cnt = 1
inbf_cmdgen_regrd_cnt = 1
inbf_cmdgen_regwr_cnt = 302068967
inbf_rx_err0_pkt_cnt = 0
inbf_rx_err1_pkt_cnt = 0
inbf_rx_err2_pkt_cnt = 0
inbf_rx_err3_pkt_cnt = 0
inbf_rx_err4_pkt_cnt = 0
inbf_exec_cmd_err_cnt = 0
inbf_wdata_err_cnt = 0
inbf_act_tbl_timeout_cnt = 0
cla_ipsec_sn_tbl_parerr_pkt_cnt = 0
stat_fifo_parerr_pkt_cnt = 0
stat_ag_ram_dbiterr_pkt_cnt = 0
stat_acc_ram_dbiterr_pkt_cnt = 0
stat_ddr_rl_ram_dbiterr_pkt_cnt = 0
stat_ag_ram_sbiterr_pkt_cnt = 0
stat_acc_ram_sbiterr_pkt_cnt = 0
stat_ddr_rl_ram_sbiterr_pkt_cnt = 0
inbs_ram_dbiterr_cnt = 0
stat_in_rx_pkt_cnt = 0
acc_cache_access_col_cnt = 0
acc_cache_insert_fail_cnt = 0
acc_cache_replace_cnt = 0
acc_cache_cpu_col_cnt = 0
ddr_rx_pkt_cnt = 0
ddr_rl_cache_insert_fail_cnt = 0
ddr_rl_cache_insert_update_cnt = 0
ddr_read_cnt = 0
ddr_write_cnt = 0
inbs_rx_request_pkt_cnt = 0
inbs_tx_response_pkt_cnt = 0
inbs_stat_collect_cnt = 0
inbs_rx_err0_pkt_cnt = 0
inbs_rx_err1_pkt_cnt = 0
inbs_rx_err2_pkt_cnt = 0
inbs_rx_err3_pkt_cnt = 0
inbs_rx_err4_pkt_cnt = 0
inbs_exec_cmd_err_cnt = 0
inbs_stat_collect_timeout_err_cnt = 0
key_tbl_dbiterr_pkt_cnt = 0
ts_tbl_dbiterr_pkt_cnt = 0
act_tbl_sbiterr_pkt_cnt = 0
act_tbl_dbiterr_pkt_cnt = 0

module: kc25-ingress-pkt-processor, pipe: 0
-------------------------------------------
proc_pkt_in_cnt = 964
proc_nic_pkt_out_cnt = 964
proc_egr_pkt_out_cnt = 0
proc_ilk_pkt_out_cnt = 0
proc_cap_be_pkt_out_cnt = 0
proc_cap_ae_pkt_out_cnt = 0
proc_cap_tail_drop_cnt = 0
proc_instr_drop_pkt_cnt = 0
proc_err_ar_drop_pkt_cnt = 0
```

```
proc_pkt_in_fifo_sbiterr_pkt_cnt = 0
proc_pkt_in_fifo_dbiterr_pkt_cnt = 0
proc_rwe_data_fifo_sbiterr_pkt_cnt = 0
proc_rwe_data_fifo_dbiterr_pkt_cnt = 0
proc_pkt_out_fifo_sbiterr_pkt_cnt = 0
proc_pkt_out_fifo_dbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cks_chk_tcp_udp_err_pkt_cnt = 0
proc_cks_chk_ip_err_pkt_cnt = 0
proc_cks_chk_both_err_pkt_cnt = 0

module: kc25-ingress-pkt-parser, pipe: 0
----------------------------------------
par_hi_pri_q_good_pkt_cnt = 0
par_hi_pri_q_err_pkt_cnt = 0
par_hi_pri_q_taildrop_pkt_cnt = 0
par_md_pri_q_good_pkt_cnt = 0
par_md_pri_q_err_pkt_cnt = 0
par_md_pri_q_taildrop_pkt_cnt = 0
par_lo_pri_q_good_pkt_cnt = 964
par_lo_pri_q_err_pkt_cnt = 0
par_lo_pri_q_taildrop_pkt_cnt = 0
par_hi_pri_q_sbiterr_pkt_cnt = 0
par_hi_pri_q_dbiterr_pkt_cnt = 0
par_md_pri_q_sbiterr_pkt_cnt = 0
par_md_pri_q_dbiterr_pkt_cnt = 0
par_lo_pri_q_sbiterr_pkt_cnt = 0
par_lo_pri_q_dbiterr_pkt_cnt = 0

module: kc25-egress-scheduler, pipe: 0
---------------------------------------
egr_rx_ingr_good_pkt_cnt = 0
egr_rx_octeon_good_pkt_cnt = 0
egr_rx_all_good_pkt_cnt = 0
egr_rx_ingr_err_pkt_cnt = 0
egr_rx_octeon_err_pkt_cnt = 0
egr_rx_ingr_drop_pkt_cnt = 0
egr_rx_octeon_drop_pkt_cnt = 0
egr_tx_ingr_pkt_cnt = 0
egr_tx_octeon_pkt_cnt = 0
egr_tx_all_pkt_cnt = 0
egr_ingr_pktbuf_ecc_sbiterr_cnt = 0
egr_ingr_pktbuf_ecc_dbiterr_cnt = 0
egr_ingr_schefifo_ecc_sbiterr_cnt = 0
egr_ingr_schefifo_ecc_dbiterr_cnt = 0
egr_octeon_pktbuf_ecc_sbiterr_cnt = 0
egr_octeon_pktbuf_ecc_dbiterr_cnt = 0
egr_octeon_schefifo_ecc_sbiterr_cnt = 0
egr_octeon_schefifo_ecc_dbiterr_cnt = 0


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

======================      show asp drop       ======================

Frame drop:
  Slowpath security checks failed (sp-security-failed)                    148
  FP L2 rule drop (l2_acl)                                                493
  Interface is down (interface-down)                                        2

Last clearing: Never
```

```
Flow drop:

Last clearing: Never

======================  show interface detail   ======================

Interface Ethernet1/1 "outside", is down, line protocol is down
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
 Full-Duplex, 1000 Mbps
 MAC address 6c13.d509.5194, MTU 1500
 IP address unassigned
 Auto-Negotiation is turned on
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 packets output, 0 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
  Traffic Statistics for "outside":
 0 packets input, 0 bytes
 0 packets output, 0 bytes
 0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 5
 Interface config status is active
 Interface state is not active
```

show pager

要显示CLI会话的当前页面长度，即在输出暂停并显示--More--指示之前显示的行数，请使用**show pager** 命令。

show pager

注释 不能为 threat defense CLI 设置页面长度。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show pager** 命令的输出示例。由于您无法在 threat defense CLI 中设置页面长度，因此输出指示没有分页程序。

```
> show pager
no pager
```

show packet debugs

要从数据库中检索和查看存储的调试日志，请使用 **show packet debugs** 命令。在某些版本中，此命令可能带有连字符： **show packet-debugs**

show packet debugs ［ **match** ［ *protocol* ］ ［ *source-ip* ］［ *source-port* ］［ *dest-ip* ］ ［ *dest-port* ］［ **module** *module-id* ］ ［ **packet-id** *packet-id* ］ ［ **severity** *0-7* ］［ **time-start** *time* ］ ［ **time-end** *time* ］］

Syntax Description

match	匹配为过滤连接而输入的以下一个或多个选项：源IP、目的IP、源端口、目标端口或协议。
protocol	协议的名称。
source-ip	源 IP 地址。
source-port	源端口号。
dest-ip	目标 IP 地址。
dest-port	目标端口号。
module *module-id*	用于过滤调试日志的模块名称。
packet-id *packet-id*	用于过滤调试日志的唯一数据包 ID。
severity *0-7*	以下严重性级别之一： • 0（应急） - 系统不可用 • 1（警报）- 需要立即采取措施 • 2（严重）- 严重情况 • 3（错误） - 错误情况 • 4（警告） - 警告情况 • 5（通知） - 正常，但重大的情况 • 6（说明性） - 仅信息性消息 • 7（调试） - 仅调试消息
time-start *time*	返回指定开始时间之后的所有日志。
time-end *time*	返回指定时间之前的所有日志。

Command History

版本	修改
6.4	引入了此命令。

使用指南

使用 **show packet debugs** 命令从数据库中检索和查看存储的调试日志。

[] 中的所有关键字都是可选的。如果未输入特定关键字，则该关键字将被视为 any。所有调试都按时间戳的升序显示。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> show packet debugs
```

Related Commands

命令	Description
debug	启用调试。

show parser dump

show parser dump 命令供内部或思科技术支持使用。

show password encryption

要显示密码加密配置设置，请使用 **show password encryption** 命令。

show password encryption

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 不允许配置主密码加密，因此此命令应始终显示密码加密已禁用，并且未设置主密钥散列。

如果密钥已保存，则密钥散列旁边会显示“已保存”。如果没有密钥或者密钥已从运行配置中删除，将会显示“Not set”而不是哈希值。

示例

以下是 **show password encryption** 命令的输出示例：

```
> show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
```

show path-monitoring

要显示有关路径监控输出的信息，请使用 **show path monitoring** 命令。

show path-monitoring ［ **interface** *name* ］［ **detail** ］

Syntax Description

Interface*name*	显示路径监控指标的接口
detail	（可选）显示有关路径监控指标的详细信息。

Command Default

无默认行为或值。

Command History

版本	修改
7.1	引入命令是为了显示指定接口的路径监控详细信息。

使用指南

show path-monitoring 命令显示指定出口接口的路径监控输出。

示例

以下是 *outside 1* 接口的 **show path-monitoring** 命令的输出示例：

```
firepower# show path-monitoring interface outside1
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 1 second(s) ago
```

以下是 *outside 1* 接口的 **show path-monitoring detail** 命令的输出示例：

```
firepower#
firepower# show path-monitoring interface outside1 detail
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 8 second(s) ago

    Internal data:
        Total probes sent: 418553
        Total probes pending: 0
        Current probes pending: 0
        Current RTT sum: 51674
```

```
Current RTT square sum: 154410282
Flags: 0x2
Current queue index: 14
Index:  0, Timestamp:              0, RTT:     962
Index:  1, Timestamp:              0, RTT:    1096
Index:  2, Timestamp:              0, RTT:    1056
Index:  3, Timestamp:              0, RTT:    1457
Index:  4, Timestamp:              0, RTT:    1078
Index:  5, Timestamp:              0, RTT:    1114
Index:  6, Timestamp:              0, RTT:    1570
Index:  7, Timestamp:              0, RTT:    6865
Index:  8, Timestamp:              0, RTT:    1035
Index:  9, Timestamp:              0, RTT:    1334
Index: 10, Timestamp:              0, RTT:    1090
Index: 11, Timestamp:              0, RTT:    1099
Index: 12, Timestamp:              0, RTT:    1429
Index: 13, Timestamp:              0, RTT:    1048
Index: 14, Timestamp:              0, RTT:     985
Index: 15, Timestamp:              0, RTT:    1002
Index: 16, Timestamp:              0, RTT:    1013
Index: 17, Timestamp:              0, RTT:    1741
Index: 18, Timestamp:              0, RTT:    1231
Index: 19, Timestamp:              0, RTT:    1517
Index: 20, Timestamp:              0, RTT:    7780
Index: 21, Timestamp:              0, RTT:    1018
Index: 22, Timestamp:              0, RTT:    1036
Index: 23, Timestamp:              0, RTT:    2369
Index: 24, Timestamp:              0, RTT:    1120
Index: 25, Timestamp:              0, RTT:    1062
Index: 26, Timestamp:              0, RTT:    1088
Index: 27, Timestamp:              0, RTT:    1073
Index: 28, Timestamp:              0, RTT:    1060
Index: 29, Timestamp:              0, RTT:    1071
Index: 30, Timestamp:              0, RTT:    1116
Index: 31, Timestamp:              0, RTT:    1075
Index: 32, Timestamp:              0, RTT:    1084
```

Related Commands

命令	Description
policy-route	在接口上配置策略型路由。

show pclu

show pclu 命令供内部或思科技术支持使用。

show perfmon

要显示有关设备性能的信息，请使用 **show perfmon** 命令。

show perfmon ［**detail**］

Syntax Description

detail	（可选）显示其他统计信息。这些统计信息与思科统一防火墙 MIB 的全局和单一协议连接对象收集的统计信息相一致。

Command History

版本	修改
6.1	引入了此命令。

使用指南

perfmon 命令按定义的时间间隔持续显示性能统计信息。使用 **show perfmon** 命令可立即显示这些信息。

示例

以下是 **show perfmon detail** 命令的输出示例：

```
> show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

命令	Description
perfmon	按定义的时间间隔显示详细的性能监控信息。

show perfstats

要显示有关设备性能的统计信息，请使用 **show perfstats** 命令。

show perfstats

Command History

版本	修改
6.1	引入了此命令。

使用指南

show perfstats 命令显示检测引擎的性能信息。命令会显示可用引擎的列表，您可以选择要查看其统计信息的引擎。然后，您会看到许多配置文件；选择要查看的内容。

这些文件对管理中心远程管理的系统有意义。对于使用本地管理器设备管理器管理的系统，这些文件通常没有内容。

如果您决定不想查看完整的文件，请使用 Crtl+C 停止显示。文件内容可能很长。

示例

```
> show perfstats
Available DEs:
  1 - Primary Detection Engine (703006f4-8ff6-11e6-bb6e-8f2d5febf243)
  0 - Cancel and return to CLI

Select a DE to profile: 1
Available now files:
  1 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-13
  2 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-16
  3 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-11
  4 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-15
  5 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-14
  6 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-12
  7 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/instance-1/now
  0 - Cancel and return to DE selection

Select a now file: 7
Mon Oct 17 00:05:00 2016
                 Pkts Recv: 162
                 Pkts Drop: 0
            Block Verdicts: 0
                 Mbits/Sec: 0.001
                 Drop Rate: 0%
                Alerts/Sec: 0
          Total Alerts/Sec: 0
(...remaining content truncated...)
```

show pim bsr-router

要显示引导路由引导程序 (BSR) 信息，请使用 **show pim bsr-router** 命令。

show pim bsr-router

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show pim bsr-router** 命令的输出示例：

```
> show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

show pim df

要显示汇聚点 (RP) 或接口的双向 DF“优胜者”，请使用 **show pim df** 命令。

show pim df ［**winner**］［*rp_address* | *interface_name*］

Syntax Description

rp_address	可以是以下各项之一： • RP 的名称，如域名系统 (DNS) 主机表中所定义。 • RP 的 IP 地址。这是采用四点分十进制符号的组播 IP 地址。
interface_name	物理或逻辑接口名称。
winner	（可选）显示每个 RP 的每个接口在 DF 选定中的获胜者。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令还显示适用于 RP 的优胜衡量标准。

示例

以下是 **show pim df** 命令的输出示例：

```
> show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

要显示组到协议的映射表，请使用 **show pim group-map** 命令。

show pim group-map ［**info-source** | **rp-timers**］［*group*］

Syntax Description

group	（可选）可以是以下各项之一： • 组播组的名称，如 DNS 主机表中所定义。 • 组播组的 IPv4 或 IPV6 地址。
info-source	（可选）显示组范围信息源。
rp-timers	（可选）显示组到 RP 映射的正常运行时间和到期计时器。

Command Default

显示所有组的组-协议映射。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 RP 的所有组协议地址映射。在设备上从不同的客户端获知映射。

在设备上实施 PIM 会在映射表中填充各种特殊条目。自动 RP 组范围会从稀疏模式组范围中专门排除。SSM 组范围也不属于稀疏模式范围。链路本地组播组（224.0.0.0 至 224.0.0.225，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。最后一个条目使用给定 RP 在稀疏模式下显示所有剩余的组。

示例

以下是 **show pim group-map** 命令的输出示例：

```
> show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

在行 1 和行 2 中，自动 RP 组范围会从稀疏模式组范围中专门排除。

在行 3 中，链路本地组播组（224.0.0.0 至 224.0.0.255，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。

在行 4 中，PIM 源特定组播 (PIM-SSM) 组范围映射到 232.0.0.0/8。

最后一个条目显示，所有剩余的组都处于稀疏模式并映射到 RP 10.10.3.2。

show pim interface

要显示 PIM 的接口特定信息，请使用 **show pim interface** 命令。

show pim interface ［*interface_name* | **state-off** | **state-on**］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
state-off	（可选）显示禁用了 PIM 的接口。
state-on	（可选）显示启用了 PIM 的接口。

Command Default

如果不指定接口，将会显示所有接口的 PIM 信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 设备本身就是 PIM 邻居。因此，此命令的输出中的“邻居数”列显示的邻居数会比实际邻居数大 1。

示例

以下示例展示内部接口的 PIM 信息：

```
> show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

show pim join-prune statistic

要显示 PIM 加入/删除汇聚统计信息，请使用 **show pim join-prune statistic** 命令。

show pim join-prune statistic ［*interface_name*］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

Command Default

如果不指定接口，此命令将会显示所有接口的联接/修剪统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear pim counters** 命令清除 PIM 加入/删除统计信息。

示例

以下是 **show pim join-prune statistic** 命令的输出示例：

```
> show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received
             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

命令	Description
clear pim counters	清除 PIM 流量计数器。

show pim neighbor

要显示 PIM 邻居表中的条目，请使用 **show pim neighbor** 命令。

show pim neighbor ［**count** | **detail**］［*interface*］

Syntax Description

interface	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
count	（可选）显示 PIM 邻居总数以及每个接口的 PIM 邻居数。
detail	（可选）显示通过上游检测问候选项获知的邻居的其他地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令用于确定路由器通过 PIM 问候消息获知的 PIM 邻居。此外，此命令还指明哪个接口是指定路由器 (DR) 以及邻居何时能够双向运行。

threat defense 设备本身就是 PIM 邻居。因此， threat defense 接口会显示在此命令的输出中。 threat defense 设备的 IP 地址旁边带有一个星号。

示例

以下是 **show pim neighbor** 命令的输出示例：

```
> show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

show pim range-list

要显示 PIM 的范围列表信息，请使用 **show pim range-list** 命令。

show pim range-list ［**config**］［*rp_address*］

Syntax Description

config	显示 PIM CLI 范围列表信息。
rp_address	可以是以下各项之一： • 汇聚点 (RP) 的名称，如域名系统 (DNS) 主机表中所定义。 • RP 的 IP 地址。这是采用四点分十进制符号的组播 IP 地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令用于确定组映射的组播转发模式。此命令的输出还指明范围的集合点(RP)地址（如果适用）。

示例

以下是 **show pim range-list** 命令的输出示例：

```
> show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

命令	Description
show pim group-map	显示组到 PIM 模式的映射和活动 RP 信息。

show pim topology

要显示 PIM 拓扑表信息，请使用 **show pim topology** 命令。

show pim topology ［**reserved** | **route-count** ［**detail**］ | *group* ［*source*］］

Syntax Description

reserved	显示保留组的 PIM 拓扑表信息。
route-count	显示 PIM 拓扑表中的路由数量。
detail	（可选）显示每个组更详细的计数信息。
group	（可选）可以是以下各项之一： • 组播组的名称，如 DNS 主机表中所定义。 • 组播组的 IPv4 或 IPV6 地址。
source	（可选）可以是以下各项之一： • 组播源的名称，如 DNS 主机表中所定义。 • 组播源的 IPv4 或 IPV6 地址。

Command Default

显示所有组和源的拓扑信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 PIM 拓扑表可显示给定组、(*, G)、(S, G) 和 (S, G)RPT（它们分别有自己的接口列表）的各个条目。

PIM 通过 MRIB 传达这些条目的内容；MRIB 是组播路由协议（例如 PIM）、本地成员协议（例如互联网组管理协议 [IGMP]）和系统的组播转发引擎之间的通信中介。

MRIB 显示对于给定 (S, G) 条目应在哪个接口接收数据包以及应在哪个接口转发数据包。此外，在转发过程中会使用组播转发信息库 (MFIB) 表，以决定每个数据包的转发操作。

注释 有关转发信息，请使用 **show mfib route** 命令。

示例

以下是 **show pim topology** 命令的输出示例：

```
> show pim topology
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

以下是 **show pim topology reserved** 命令的输出示例：

```
> show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

以下是 **show pim topology route-count** 命令的输出示例：

```
> show pim topology route-count
PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

命令	Description
show mrib route	显示 MRIB 表。

show pim traffic

要显示 PIM 流量计数器，请使用 **show pim traffic** 命令。

show pim traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear pim counters** 命令清除 PIM 流量计数器。

示例

以下是 **show pim traffic** 命令的输出示例：

```
> show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                        0        9485
Hello                                    0        9485
Join-Prune                               0           0
Register                                 0           0
Register Stop                            0           0
Assert                                   0           0
Bidir DF Election                        0           0

Errors:
Malformed Packets                                    0
Bad Checksums                                        0
Send Errors                                          0
Packet Sent on Loopback Errors                       0
Packets Received on PIM-disabled Interface           0
Packets Received with Unknown PIM Version            0
```

Related Commands

命令	Description
clear pim counters	清除 PIM 流量计数器。

show pim tunnel

要显示有关 PIM 隧道接口的信息，请使用 **show pim tunnel** 命令。

show pim tunnel ［*interface_name*］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

Command Default

如果不指定接口，此命令会显示所有接口的 PIM 隧道信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

PIM 注册数据包通过虚拟封装隧道接口从源第一跳 DR 路由器发送到交汇点 (RP)。在 RP 上，虚拟解封隧道用于代表 PIM 注册数据包的接收接口。此命令显示这两种接口的隧道信息。

注册隧道是通过共享树从源发送到 RP 以供分布的（PIM 注册消息中的）封装组播数据包。注册仅适用于 SM，而不适用于 SSM 和双向 PIM。

示例

以下是 **show pim tunnel** 命令的输出示例：

```
> show pim tunnel

Interface     RP Address    Source Address

Encapstunne   l0 10.1.1.1   10.1.1.1
Decapstunne   l0 10.1.1.1   -
```

Related Commands

命令	Description
show pim topology	显示 PIM 拓扑表。

show policy-list

要显示有关已配置的策略列表和策略列表条目的信息，请使用 **show policy-list** 命令。

show policy-list ［*policy_list_name*］

Syntax Description

policy_list_name	（可选）显示有关指定策略列表的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

策略列表在 BGP 路由中用作路由地图的匹配条件。

示例

以下是 **show policy-list** 命令的输出示例：

```
> show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1

policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

show policy-route

要显示基于策略的路由配置，请使用 **show policy-route** 命令。

show policy-route

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show policy-route** 命令的输出示例：

```
> show policy-route
Interface Route map
GigabitEthernet0/0   equal-access
```

show port-channel

要以详细的单行摘要形式显示 EtherChannel 信息，或显示端口和端口通道信息，请使用 **show port-channel** 命令。

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

Syntax Description

brief	（默认设置）显示简要信息。
channel_group_number	（可选）指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
detail	（可选）显示详细信息。
port	（可选）显示每个接口的信息。
protocol	（可选）显示 EtherChannel 协议，例如 LACP（如果已启用）。
summary	（可选）显示端口通道摘要。

Command Default

默认值为 **brief**。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show port-channel** 命令的输出示例：

```
> show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

以下是 **show port-channel summary** 命令的输出示例：

```
> show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
```

```
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

以下是 **show port-channel detail** 命令的输出示例：

```
> show port-channel detail
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip

       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
```

```
Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel port** 命令的输出示例：

```
> show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
```

```
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d

Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel protocol** 命令的输出示例：

```
> show port-channel protocol
        Channel-group listing:
        ----------------------
Group: 1
----------
Protocol: LACP
```

Related Commands

命令	Description
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel load-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

show port-channel load-balance

对于 EtherChannel，要显示当前的端口信道负载平衡算法，或者要查看为给定参数集选择的成员接口，请使用 **show port-channel load-balance** 命令。

show port-channel *channel_group_number* **load-balance** [**hash-result** {{**ip** | **ipv6** | **mac** | **l4port** | **mixed**} *parameters* | **vlan-only** *number*}]

Syntax Description

channel_group_number	指定 EtherChannel 信道组编号（1 到 48）。
hash-result	（可选）显示在为当前负载平衡算法输入的散列值之后选择的成员接口。
ip	（可选）指定 IPv4 数据包参数。
ipv6	（可选）指定 IPv6 数据包参数。
l4port	（可选）指定端口数据包参数。
mac	（可选）指定 MAC 地址数据包参数。
mixed	（可选）指定 IP 或 IPv6 参数的组合以及端口和/或 VLAN ID。
parameters	（可选）数据包参数（取决于类型）。例如，对于 ip，可以指定源 IP 地址、目标 IP 地址和/或 VLAN ID。
vlan-only *number*	（可选）指定数据包的 VLAN ID，范围为 0-4095。

Command History

版本	修改
6.1	引入了此命令。

使用指南

默认情况下，设备根据数据包的源 IP 地址和目标 IP 地址 (**src-dst-ip**) 来均衡接口上的数据包负载。

使用此命令可查看当前负载平衡算法；如果与 **hash-result** 关键字结合使用，此命令还可以测试将为带有给定参数的数据包选择哪个成员接口。此命令仅测试当前负载平衡算法。例如，如果算法是 src-dst-ip，请输入 IPv4 或 IPv6 源 IP 地址和目标 IP 地址。如果您输入当前算法没有使用的其他参数，这些参数将被忽略，且当前算法实际使用的而您没有输入的值将会默认为 0。例如，如果算法是 vlan-src-ip，请输入：

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

如果您输入以下内容，则 vlan-src-ip 算法会假设使用的是源 IP 地址 0.0.0.0 和 VLAN 0，并会忽略您输入的值：

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

示例

以下是 **show port-channel 1 load-balance** 命令的输出示例：

```
> show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 匹配：

```
> show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination 10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 不匹配，且使用的散列值为 0：

```
> show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

Related Commands

命令	Description
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。

show power inline

对于带 PoE 接口的型号，使用 **show power inline** 命令显示接口的电源状态。

注释 仅支持 Firepower 1010。

show power inline

Command History

版本	修改
6.5	引入了此命令。

使用指南

可以使用 PoE 接口连接需要电源的设备，例如 IP 电话或无线接入点。对于 Firepower 1010，以太网 1/7 和 1/8 支持 PoE+。

示例

以下是 Firepower 1010 的 **show power inline** 命令的输出示例：

```
> show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

下表显示每个字段的说明：

表 1: show power inline Fields

字段	Description
Interface	显示 threat defense上的所有接口（包括没有 PoE 可用的接口）。
Power	显示电源是否已开启。如果设备不需要电源，或者该接口上没有设备，或者接口已关闭，则值为 Off。如果接口不支持 PoE，则值为 n/a。
Class	显示所连接设备的 PoE 类。
Current (mA)	显示正在使用的电流。
Voltage (V)	显示正在使用的电压。

show prefix-list

要列出配置为匹配 IPv4 流量的前缀列表，请使用 **show prefix-list** 命令。

show prefix-list ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

Syntax Description

detail	显示有关前缀列表的详细信息。
summary	显示前缀列表摘要。
prefix_list_name	前缀列表的名称。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。
network/length [**longer** | **first-match**]	（可选）显示使用此网络地址和网络掩码长度（以位为单位）的指定前缀列表中的所有条目。网络掩码的长度可以是 0 到 32。 您可以选择包含以下关键字之一： • **longer** 显示与给定 network/length 匹配或比其更具体的指定前缀列表的所有条目。 • **first-match** 显示与给定 network/length 匹配的指定前缀列表的第一个条目。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是带有名为 "test" 的前缀列表的 **show prefix-list** 命令的输出示例：

```
> show prefix-list detail test

prefix-list test:   Description: test-list
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3

   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

命令	Description
clear prefix-list	重置 IP 前缀列表的命中计数。
show bgp prefix-list	显示在边界网关协议情景下有关前缀列表或前缀列表条目的信息。
show ipv6 prefix-list	显示有关 IPv6 前缀列表的信息。

show priority-queue

要显示某个接口的优先级队列配置或统计信息，请使用 **show priority-queue** 命令。

show priority-queue {**config** | **statistics**} [*interface_name*]

Syntax Description

config	显示接口优先级队列的队列和 TX 环限制。
interface_name	（可选）指定要显示配置或尽力而为队列和低延迟队列详细统计信息的接口的名称。
statistics	显示尽力而为和低延迟队列的统计详细信息。

Command History

版本	修改
6.3	引入了此命令。

示例

此示例显示名为 test 的接口的统计信息。在以下输出中，BE 表示“尽力而为”队列，LLQ 表示低延迟队列：

```
> show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
```

以下示例显示所有已配置接口上的优先级队列的配置。

```
> show priority-queue config

Priority-Queue Config interface inside
                current          default          range
queue-limit     0                2048             0 - 2048
tx-ring-limit   4294967295               511              3 - 511

Priority-Queue Config interface test
                current          default          range
queue-limit     0                2048             0 - 2048
```

```
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface outside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface bgmember1
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
```

命令	Description
clear priority-queue statistics	将优先级队列统计信息重置为零。

show processes

要显示设备上正在运行的流程列表，请使用 **show processes** 命令。

show processes ［**cpu-hog** | **cpu-usage** ［**non-zero**］［**sorted**］ | **internals** | **memory** | **system**］

Syntax Description

cpu-hog	显示正在大量占用 CPU（即使用 CPU 超过 100 毫秒）的流程的数量及详细信息。
cpu-usage	显示在最近的 5 秒、1 分钟和 5 分钟内每个流程的 CPU 使用率。
internals	显示每个流程的内部详细信息。
memory	显示每个流程的内存分配。
non-zero	（可选）显示 CPU 使用率不是 0 的流程。
sorted	（可选）显示已排序的流程 CPU 使用率。
system	（可选）显示有关系统上当前运行的流程的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

流程是只需要几个指令的轻量级线程。 **show processes** 命令显示设备上正在运行的流程列表，如下所示：

命令	显示的数据	Description
show processes	PC	程序计数器。
show processes	SP	堆栈指针。
show processes	省/自治区	线程队列的地址。
show processes	运行时间	线程根据 CPU 时钟周期已运行的毫秒数。对于基于 CPU 时钟周期（小于 10 纳秒分辨率）而非时钟计时周期（10 毫秒分辨率）的完整、准确的流程 CPU 使用率计算，准确性达到 1 毫秒以内。
show processes	SBASE	堆栈基址。
show processes	产品	当前使用中的字节数以及堆栈的总大小。
show processes	流程	线程的功能。
show processes cpu-usage	MAXHOG	最大 CPU 大量占用运行时间，以毫秒为单位。

命令	显示的数据	Description
show processes cpu-usage	NUMHOG	CPU 大量占用运行次数。
show processes cpu-usage	LASTHOG	上一次 CPU 大量占用运行时间，以毫秒为单位。
show processes cpu-usage	PC	CPU 占用流程的指令指针。
show processes cpu-usage	Traceback	CPU 大量占用流程的堆栈跟踪。最多可回溯 14 个地址。
show processes internals	Invoked Calls	调度程序运行流程的次数。
show processes internals	Giveups	流程将 CPU 归还给调度程序的次数。

使用 **show processes cpu-usage** 命令可缩小设备上可能正在使用 CPU 的特定流程的范围。您可以使用 **sorted** 和 **non-zero** 命令进一步自定义 **show processes cpu-usage** 命令的输出。

借助调度程序和总摘要行，您可以连续运行两个 **show proccesses** 命令，并比较输出以确定：

- CPU 占用率。
- 每个线程的CPU使用率（通过将具体线程的运行时间增量与总运行时间增量作比较来确定）。

设备作为具有许多不同执行线程的单个流程运行。此命令的输出实际上显示了每个线程的内存分配和可用内存。由于这些线程协同处理与设备操作相关的数据流和其他操作，因此一个线程可能会分配内存块，而另一个线程可能会释放该内存块。输出的最后一行包含所有线程的总数。通过监控分配和可用内存之间的差异，仅此行可用于跟踪潜在的内存泄漏。

示例

以下示例展示如何显示正在运行的流程的列表：命令输出自动换行。

```
> show processes
    PC                 SP                 STATE                 Runtime               SBASE

Stack Process TID
Mwe 0x00007f9ae994881e 0x00007f9acb9d6e18 0x00007f9b027e1340          0 0x00007f9acb9cf030
32000/32768 zone_background_idb 140
Mwe 0x00007f9ae91d64ae 0x00007f9ae7659cd8 0x00007f9b027e1340          0 0x00007f9ae7652030
27568/32768 WebVPN KCD Process 14
Msi 0x00007f9aea3f8c04 0x00007f9acba86e48 0x00007f9b027e1340       2917 0x00007f9acba7f030
29944/32768 vpnlb_timer_thread 131
```

以下示例显示如何列出系统流程。

```
> show processes system
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23302 root       0 -20 1896m 558m 101m S  198  7.1  16939:07 lina
 8330 admin     20   0 15240 1188  852 R    2  0.0   0:00.01 top
23148 root      20   0 29780 2876 1268 S    2  0.0  41:27.25 UEChanneld
(...output truncated...)
```

以下示例展示如何显示每个流程的 CPU 使用率：

```
> show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00007f9ae8abcc76   0x00007f9ad04cf7a0     0.2%     0.0%     0.0%   Environment Monitor
Process
```

以下示例展示如何显示正在大量占用 CPU 的流程的数量及详细信息：

```
> show processes cpu-hog
Process:      cli_xml_server, NUMHOG: 12, MAXHOG: 30, LASTHOG: 2
LASTHOG At:   17:37:08 UTC Oct 28 2016
PC:           0x00007f9ae9b11539 (suspend)
Call stack:   0x00007f9ae9b11539  0x00007f9ae9caf084  0x00007f9ae9caf9d0
              0x00007f9ae8736425  0x00007f9ae9b13346  0x00007f9ae9b15ab4
              0x00007f9ae8730ead  0x00007f9ae87663ec  0x00007f9ae6eccde0
              0x00007f9ac4a46120  0x31223d646920696c
(...output truncated...)
```

以下示例展示如何显示每个流程的内存分配：

```
> show processes memory

------------------------------------------------------------------------------
Allocs      Allocated             Frees       Freed                 Process
             (bytes)                           (bytes)
------------------------------------------------------------------------------
0           0                     0           0                     *System Main*
0           0                     0           0                     QoS Support Module
0           0                     0           0                     SSL
0           0                     0           0                     vpnfol_thread_sync
22          8636                  78          3728                  DHCP Network Scope
Monitor
7           40459                 0           0                     Integrity FW Task
0           0                     0           0                     uauth_urlb clean
2           64                    0           0                     arp_timer
8450        233220                0           0                     HDD Health Monitor
14638       1659384               14509       1570750               PTHREAD-23518
0           0                     6           1926                  DHCP Client
(...output truncated...)
```

以下示例展示如何显示每个流程的内部详细信息：

```
> show processes internals
     Invoked      Giveups  Max_Runtime  Process
           1            0        0.002  zone_background_idb
           2            0        0.163  WebVPN KCD Process
      507512            0        0.060  vpnlb_timer_thread
           2            0        0.057  vpnlb_thread
     2029820            0        0.130  vpnfol_thread_unsent
      507455            0        0.137  vpnfol_thread_timer
(...output truncated...)
```

show process-tree

要以树关系显示系统流程，请使用 **show process-tree** 命令。

show process-tree

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令的输出主要供思科技术支持人员使用。

示例

以下是显示流程树的示例。

```
> show process-tree
init(1)-+-acpid(23138)
        |-agetty(23726)
        |-crond(23141)
        |-dbus-daemon(23119)
        |-login(23727)---clish(6394)
        |-nscd(14445)-+-{nscd}(14448)
        |             |-{nscd}(14449)
        |             |-{nscd}(14450)
        |             |-{nscd}(14451)
        |             |-{nscd}(14452)
        |             `-{nscd}(14453)
(...remaining output truncated...)
```

show ptp

要显示精确时间协议 (PTP) 统计信息和时钟信息，请使用 **show ptp** 命令。

show ptp {**clock** | **port** [*interface_name*]}

Syntax Description

clock	显示 PTP 时钟属性。
port [*interface_name*]	显示接口的PTP端口信息。您可以选择指定接口名称，以仅查看有关该接口的信息。

Command History

版本	修改
6.5	引入了此命令。

示例

以下示例显示未配置 PTP。PTP 数据包可以通过设备，但设备不使用 PTP 时钟。

```
> show ptp clock
 No clock information is available in PTP forwarding mode.
> show ptp port
 No clock information is available in PTP forwarding mode.
```

以下示例显示了 PTP 时钟属性：

```
> show ptp clock
PTP CLOCK INFO
PTP Device Type: Transparent Clock
Operation mode: One Step
Clock Identity: 0:8:2F:FF:FE:E8:43:81
Clock Domain: 0
Number of PTP ports: 4
```

以下示例显示所有启用 PTP 的接口的 PTP 端口信息：

```
> show ptp port
PTP PORT DATASET: GigabitEthernet1/1
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 1
PTP version: 2
Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 2
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 3
```

```
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 4
PTP version: 2
Port state: Enabled
```

show quota

要显示当前会话的配额统计信息，请使用 **show quota** 命令。

show quota ［**management-session**］

Syntax Description

management-session	显示当前管理会话的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您无法在 threat defense上配置管理会话配额。此命令应始终显示无限制。

示例

以下示例显示配额统计信息。

```
> show quota
quota management-session limit 0
quota management-session warning level 0
quota management-session level 0
quota management-session high water 0
quota management-session errors 0
quota management-session warnings 0
```

show raid

要查看 RAID 中 SSD 的状态，请使用 **show raid** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

show raid

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示了 RAID 中的两个 SSD：

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     0
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                  nvme1n1
Disk State:                   in-sync
Disk Slot:                    2
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

以下示例显示了 RAID 中的一个 SSD； disk2 不存在，并且 RAID 显示为“已降级”：

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  degraded
Presence:                     equipped
Lifecycle:                    available
Drive State:                  degraded
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     1
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

Related Commands

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

show random-password, random-strong-password

要生成可在更改密码时使用的密码，请使用以下命令之一

show { **random-password** | **random-strong-password** } *length*

Syntax Description

random-password	生成不包含特殊字符的随机密码。
random-strong-password	生成强随机密码，即包含特殊字符的密码。
length	指定要生成的密码的长度，8-127 个字符。

Command History

版本	修改
7.0	引入了此命令。

使用指南

生成密码仅适用于FXOS平台。如果您不想设置自己的密码，可以将这些命令与更改密码结合使用。

输入命令后，系统将显示随机密码。您可以复制/粘贴或记下密码。在任何类型的下一次按键时，密码将从输出中擦除，以便其他用户无法获取密码。

示例

以下示例显示如何使用生成的密码更改 joeuser 的密码。首先，使用 **show user** 确定最小密码长度以及是否需要强密码。在这种情况下，最小长度 (MinL) 为 8 个字符，密码强度 (Str) 为“已启用”。接下来，我们将生成 12 个字符的强密码（超过最小长度）。将其复制到剪贴板，然后将其粘贴到更改密码命令中，当更改另一个用户的密码时为 **configure user password**，当更改您登录的账户的密码时则为 **configure password**。

```
> show user
Login       UID   Auth Access  Enabled Reset   Exp  Warn    Grace MinL Str Lock Max
joeuser    1001  Local Config  Enabled   Yes   180     7  Disabled    8 Ena   No   5
> show random-strong-password 12
4j9@!GEhnL>V
> configure user password joeuser
Enter new password for user joeuser: <paste not shown>
Confirm new password for user joeuser: <paste not shown>
```

以下示例显示了尝试在非 FXOS 平台上或 FXOS 版本不支持随机密码生成的 FXOS 平台上生成密码时所看到的内容。

```
> show random-strong-password 12
Password generator is not available.
```

命令	Description
configure password	设置已登录用户的密码。

命令	Description
configure user minpasswdlength	添加新用户。
configure user password	为指定用户设置密码。
configure user strength-check	设置强密码要求。
show user	显示用户账号。

show resource types

要查看设备跟踪使用情况的资源类型，请使用 **show resource types** 命令。

show resource types

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示资源类型：

```
> show resource types
Rate limited resource types:
  Conns                     Connections/sec
  Inspects                  Inspects/sec
  Syslogs                   Syslogs/sec

Absolute limit types:
  Conns                     Connections
  Hosts                     Hosts
  IPSec                     IPSec Mgmt Tunnels
  Mac-addresses             MAC Address table entries
  ASDM                      ASDM Connections
  SSH Client                SSH Client Sessions
  SSH Server                SSH Server Sessions
  Storage                   Storage Limit Size of context directory in MB
  Telnet                    Telnet Sessions
  Xlates                    XLATE Objects
  Routes                    Routing Table Entries
  All                       All Resources
  Other VPN Sessions        Other VPN Sessions
  Other VPN Burst           Allowable burst for Other VPN Sessions
  AnyConnect                AnyConnect Premium licensed sessions
  AnyConnect Burst          Allowable burst for AnyConnect Premium licensed sessions
  IKEv1 in-negotiation      Allowable in negotiation IKEv1 SAs
```

Related Commands

命令	Description
clear resource usage	清除资源使用统计信息
show resource usage	显示设备的资源使用情况。

show resource usage

要在多模式 或每个情景的资源使用情况，请使用 **show resource usage** 命令。

show resource usage ［**all** | **detail**］［**resource** {［**rate**］ *resource_name* | **all**}］［**counter** *counter_name* ［*count_threshold*］］

Syntax Description

all	所有类型。
count_threshold	设置要显示资源须达到的资源使用量下限。默认值为 1。如果资源的使用率低于所设置的数字，则不会显示资源。如果为计数器名称指定 all，则 count_threshold 适用于当前使用情况。要显示所有资源，请将 count_threshold 设置为 0。
counter *counter_name*	显示以下计数器类型的计数： • **current**- 显示活动并发实例数或资源的当前使用率。 • **peak**- 显示自上一次清除统计信息（使用 **clear resource usage** 命令或由于设备重启）以来，峰值并发实例数或资源的峰值使用率。 • **denied**- 显示由于超过 Limit 列中所示的资源限制而被拒绝的实例的数量。 • **all**-（默认）显示所有统计信息。
detail	显示所有资源（包括不能管理的资源）的使用情况。例如，可以查看 TCP 拦截次数。
resource {[**rate**] *resource_name* | **all**}	显示特定资源的使用情况。为所有资源指定 **all** 。指定使用率可显示资源的使用率。按使用率衡量的资源包括 **conns**、 **inspects**和 **syslogs**。对于这些资源类型，必须指定 **rate** 关键字。 **conns** 资源也可以按并发连接数来测量；要查看每秒连接数，必须使用 rate 关键字。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

使用 **resource** 关键字时，资源包括以下类型：

- **asdm**- threat defense不支持与此关键字相关的功能。
- **conns**—任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。
- **hosts**- 可以通过 threat defense 设备连接的主机。
- **ipsec**- IPSec 管理隧道

- **mac-addresses**-对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
- **rate**- 按使用率测量的资源。指定 **conns**、 **inspects**或 **syslogs**。
- **routes**-路由表条目。
- **ssh**-SSH 会话。
- **storage**-情景目录 (以 MB 为单位)。
- **telnet**-Telnet 会话。
- **vpn** - VPN 资源。
- **vpn anyconnect**-AnyConnect 高级许可证限制。
- **vpn ikev1 in-negotiation**- 可以协商的 IKEv1 会话数。
- **VPN Other** - 站点间 VPN 会话。
- **VPN Burst Other** - 站点间 VPN 突发会话。
- **xlates**—NAT 转换。

示例

以下是 **show resource usage** 命令的样本输出，其中显示所有资源的资源使用情况。设备处于单情景模式，因此情景显示为系统。

```
> show resource usage
Resource                Current         Peak      Limit         Denied Context
Syslogs [rate]                0          144        N/A              0 System
Conns                         0            5     100000              0 System
Xlates                        0            5        N/A              0 System
Hosts                         0            8        N/A              0 System
Conns [rate]                  0            1        N/A              0 System
Inspects [rate]               0            3        N/A              0 System
Mac-addresses                 0            4      16384              0 System
Routes                        9            9  unlimited              0 System
```

Related Commands

命令	Description
clear resource usage	清除资源使用统计信息
show resource types	显示资源类型列表。

show rip database

要显示 RIP 拓扑数据库中存储的信息，请使用 **show rip database** 命令。

show rip database ［*ip_addr* ［*mask*］］

Syntax Description

ip_addr	（可选）限制要为指定网络地址显示的路由。
mask	（可选）指定可选网络地址的网络掩码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

RIP 数据库包含通过 RIP 获知的所有路由。在该数据库中出现的路由不一定出现在路由表中。

示例

以下是 **show rip database** 命令的输出示例：

```
> show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

以下是 **show rip database** 命令的输出示例，其中包含网络地址和网络掩码：

```
> show rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

show rollback-status

要显示从 管理中心发送的最新回滚作业（如有）的状态，请使用 **show rollback-status** 命令。

show rollback-status

Command History

版本	修改
6.3	引入了此命令。

使用指南

如果 管理中心 需要在部署作业期间回滚配置更改，它会向设备发送请求，然后重置 管理中心 与设备的管理连接。您可以使用此命令查看回滚作业的状态。

回滚作业仅与运行配置文件中配置的命令相关；它不会回滚 Snort 配置。

如果设备在高可用性模式下运行，请仅在主用设备上使用此命令。在集群中，只能在主设备上使用命令。

信息包括以下内容：

- 状态- 最近的回滚作业的状态。
  - 无 - 未曾请求回滚作业。
  - 正在进行 - 系统已收到回滚请求，并且正在执行回滚作业。
  - 成功 - 回滚已成功完成。
  - 已恢复 - 回滚到从 设备管理器 发送的配置失败。系统将恢复为上次保存的配置。
  - 失败 - 回滚已完成，但出现错误。
- 开始时间/结束时间 - 作业的开始和结束时间。N/A 表示没有作业；对于结束时间，N/A 也可能意味着作业仍在进行中。

示例

以下示例显示了未请求回滚作业的正常情况。

```
> show rollback-status
        Status      : None
        Start Time  : N/A
        End Time    : N/A
```

Related Commands

命令	Description
show running-config	显示在运行配置文件中定义的配置。

show route

要显示数据接口的路由表，请使用 **show route** 命令。

show route ［ **vrf** *name* ｜ **all** ］ **summary** ［ **management-only** ］ ［ **cluster** ｜ **failover** ｜ *ip_address* ［ *mask* ］ ［ **longer-prefixes** ］ ｜ **bgp** ［ *as_number* ］ ｜ **connected** ｜ **eigrp** ［ *process_id* ］ ｜ **isis** ｜ **ospf** ［ *process_id* ］ ｜ **rip** ｜ **static** ｜ **summary** ｜ **zone** ］

Syntax Description

bgp *as_number*	（可选）显示BGP路由的路由信息库(RIB)代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。AS 编号将显示限制为使用指定 AS 编号的路由条目。
cluster	（可选）显示路由信息库 (RIB) 代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。
connected	（可选）显示已连接的路由。
eigrp *process_id*	（可选）显示 EIGRP 路由。但是， threat defense 不支持 EIGRP。
failover	（可选）显示出现故障转移且备用设备变为主用设备后的当前路由表序列号和路由条目数。
interface_name	（可选）要显示使用指定接口的路由条目。
ip_address mask	（可选）显示通往指定目的地的路由。
isis	（可选）显示 IS-IS 路由。
longer-prefixes	（可选）仅显示与指定的 IP 地址/掩码对匹配的路由
management-only	（可选）显示 IPv4 管理路由表中的路由。
ospf *process_id*	（可选）显示 OSPF 路由。
rip	（可选）显示 RIP 路由。
static	（可选）显示静态路由。
summary	（可选）显示路由表的当前状态。
［**vrf***name* ｜ **all**］ **summary**	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。摘要关键字可用于查看所有 VRF 的路由信息。
zone	（可选）显示区域接口的路由。

Command History

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

使用指南

show route 命令的输出类似于 **show ipv6 route** 命令的输出，唯一不同之处是，前者显示的信息是IPv4特定信息。所示路由仅适用于数据接口，不适用于虚拟管理接口。要查看管理接口的默认网关，请使用 **show network** 命令。要查看管理接口上的路由，请使用 **show network-static-routes** 命令。

注释 除非在 threat defense 设备上配置了这些功能，否则不会显示 **clustering** 和 **failover** 关键字。

show route 命令列出可用于新连接的“最佳”路由。如果您将允许的 TCP SYN 发送到备用接口，threat defense 设备只能使用同一个接口作出响应。如果该接口上的 RIB 中没有默认路由，设备将会由于没有邻接而丢弃数据包。 **show running-config route** 命令中所示的所有配置将保留在系统的某些数据结构中。

使用 **show asp table routing** 命令可查看特定于后端接口的路由表。这一设计类似于 OSPF 或 EIGRP，其中的协议特定路由数据库不同于全局路由表，后者仅显示“最佳”路由。此行为是有意设计的行为。

示例

以下是 **show route** 命令的输出示例：

```
> show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

以下是 **show route failover** 命令的输出示例，其中显示在故障转移后 OSPF 和 EIGRP 路由与备用设备之间的同步情况：

```
> show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

以下是 **show route cluster** 命令的输出示例：

```
> show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

以下是 **show route summary** 命令的输出示例：

```
> show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

以下示例显示已启用虚拟路由和转发 (VRF) 时所有虚拟路由器中的路由。在本例中，除了首先显示的全局路由器之外，还有两个虚拟路由器（test1 和 test2）。

```
> show route all

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        192.168.0.0 255.255.255.0 is directly connected, inside1
L        192.168.0.100 255.255.255.255 is directly connected, inside1


Routing Table: test1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        10.10.10.0 255.255.255.0 is directly connected, outside
L        10.10.10.10 255.255.255.255 is directly connected, outside


Routing Table: test2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        20.20.20.0 255.255.255.0 is directly connected, inside
L        20.20.20.20 255.255.255.255 is directly connected, inside
```

以下示例显示名为 red 的虚拟路由器的路由。请注意，泄漏到其他虚拟路由器的静态路由使用密钥 SI 表示。

```
> show route vrf red

Routing Table: red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        2.1.1.0 255.255.255.0 is directly connected, gig0
L        2.1.1.2 255.255.255.255 is directly connected, gig0
S        7.0.0.0 255.0.0.0 [1/0] via 8.1.1.1, gig0
SI       11.0.0.0 255.0.0.0 [1/0] is directly connected, gig3
```

以下示例显示所有 VRF 的路由摘要。

```
> show route all summary
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           4           0           352         1184
static               1           0           0           88          296
ospf 1               0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 2                                           792
Total                    3           4           0           440         2272


Routing Table: v1
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 12              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 1                                           416
Total                    1           2           0           176         1008


Routing Table: v2
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 13              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 1                                           416
Total                    1           2           0           176         1008
```

Related Commands

命令	Description
show ipv6 route	显示 IPv6 路由表。
show vrf	显示系统上的虚拟路由器。

show route-map

要显示路由地图信息，请使用 **show route-map** 命令。

show route-map [**all** | **dynamic** [**application** [*application*] | **detail** | *route_map*] | *route_map*]

Syntax Description

all	显示有关静态和动态路由地图的信息。
dynamic	仅显示有关动态路由地图的信息。
application *application*	创建路由地图的应用。
route_map	为路由地图命名。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show route-map dynamic** 命令的输出示例：

```
> show route-map dynamic
route-map MIP-10/24/06-05:23:46.091-1-MPATH_1, permit, sequence 0, identifier 54943520
  Match clauses:
    ip address (access-lists): VOICE
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

show rule hits

要显示所有评估的访问控制策略和预过滤器策略的规则命中信息，请使用 **show rule hits** 命令。

show rule hits [**id** *number* | **raw** | **cumulative** | **node-wise**] [**gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*]

Syntax Description

cumulative	（可选。）显示所有集群或高可用性 (HA) 节点中规则命中的累计总和。命中计数是按节点计算的，因此总和显示整个集群或HA对的总命中数。
id*number*	（可选）规则的 ID。包含此参数会限制向指定规则显示的信息。指定 ID 时不能指定任何其他选项。 使用 **show access-list** 命令标识规则 ID。
node-wise	（可选。）显示集群或 HA 对中每台设备的当前命中计数。
raw	（可选）以 .csv 格式显示规则命中信息。
gt *#hit-count*	（可选）显示命中计数大于 *#hit-count*的所有规则。
lt *#hit-count*	（可选）显示命中计数小于 *#hit-count*的所有规则。
range *#hit-count1 #hit-count2*	（可选）显示命中计数介于 *#hit-count1* 和 *#hit-count2*之间的所有规则。

Command Default

如果不指定规则 ID，则会显示所有规则的规则命中信息。

Command History

版本	修改
6.4	引入了此命令。
7.2	添加了 **cumulative** 和 **node-wise** 关键字。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

查看访问控制或预过滤策略时，可以使用本地或远程设备管理器更轻松地查看规则命中信息。请注意，此命令中显示的规则命中信息基于实际规则，而不是为部分实施规则而生成的任何ACL中的任何访问控制条目 (ACE)。因此，此命令显示的命中计数信息不等同于 **show access-list** 命令显示的命中计数。

使用**show access-list** 命令标识规则ID。但是，此命令的输出中并未列出所有规则。对于管理中心受管设备，您可以对以下 URL 使用 REST API GET 操作来查看所有规则及其 ID：

- `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
- `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}`

```
/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true
```

示例

以下示例显示规则命中信息：

```
> show rule hits
RuleID            Hit Count       First Hit Time(UTC)       Last Hit Time(UTC)
--------------------------------------------------------------------------------
268436979            1            22:01:39 Jan 25 2019      22:01:39 Jan 25 2019
268436980            1            22:01:51 Jan 25 2019      22:01:51 Jan 25 2019
268436981            2            22:02:00 Jan 25 2019      22:02:02 Jan 25 2019
268436925            2            22:01:53 Jan 25 2019      22:04:51 Jan 25 2019
```

以下示例显示集群或 HA 对中所有设备的摘要命中计数。

```
> show rule hits cumulative

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------
111116               2                   10:03:55 Apr 12 2021     10:04:02 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021
111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

以下示例显示集群或 HA 对中每台设备的命中计数。为每个设备单独保存命中计数。

```
> show rule hits node-wise

Active/Control node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------
111116               1                   10:03:55 Apr 12 2021     10:03:55 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021

Standby/Data node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------

111116               1                   10:04:02 Apr 12 2021     10:04:02 Apr 12 2021

111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

Related Commands

命令	Description
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。

命令	Description
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

show running-config

要显示设备上当前运行的配置，请使用 **show running-config** 命令。

show running-config ［**all**］［*command*］

Syntax Description

all	显示整个运行配置，包括默认设置。
command	显示与特定命令关联的配置。有关可用 命令，请参阅 **show running-config ?**CLI 帮助。 **注释** threat defense 不直接支持 CLI 帮助中列出的每个命令。给定选项可能没有任何配置。某些选项只能使用 管理中心的 FlexConfig 进行配置。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show running-config 命令用于显示设备上的内存中的活动配置（包括保存的配置更改）。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，您应仅将运行配置中的信息用作故障排除辅助工具。使用 管理中心设备管理器作为分析设备配置的主要方法。

示例

以下是 **show running-config** 命令的输出示例：

```
> show running-config
: Saved

:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
:
NGFW Version 6.1.0
!
hostname firepower
enable password $sha512$5000$Col980QPR9VVq/VYoAkGJw==$ZvzuZDNpcvvEP/DGbBqytA== pbkdf2
strong-encryption-disable
names

!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
 security-level 0
 ip address 192.168.10.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 shutdown
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/2
 shutdown
 nameif dmz
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority
 Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: Initial AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_IPSEC_ACL_1 extended permit ip any6 any6
!
tcp-map UM_STATIC_TCP_MAP
```

```
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options md5 clear
  urgent-flag allow
!
no pager
logging enable
logging timestamp rfc5424
logging buffered informational
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group CSM_FW_ACL_ global
as-path access-list 2 deny 100$
as-path access-list 2 permit 200$
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no sysopt connection permit-vpn
crypto ipsec ikev1 transform-set CSM_TS_1 esp-des esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_outside_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_outside_map 1 set peer 10.10.10.10
crypto map CSM_outside_map 1 set ikev1 transform-set CSM_TS_1
crypto map CSM_outside_map 1 set reverse-route
crypto map CSM_outside_map interface outside
crypto ca trustpool policy
crypto ikev1 enable outside
crypto ikev1 policy 160
 authentication pre-share
```

```
 encryption des
 hash sha
 group 5
 lifetime 86400
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:167911f11cbf1140edeffcb0f9b17f01
: end
>
```

要查看 BFD 全局配置设置，请使用输出修饰符过滤 BFD 相关配置。以下是使用输出修饰器 **show running-config bfd** 命令的输出示例：。

```
ciscoftd# show running-config bfd
bfd map ipv4 1.1.1.1/24 1.1.1.2/32 name2
```

以下是使用输出修饰器 **show running-config bfd-template** 命令的输出示例：。

```
ciscoftd# show running-config bfd-template
bfd-template single-hop bfd_template
interval min-tx 50 min-rx 50 multiplier 3
```

```
!
bfd-template single-hop bfd_template_auth
interval min-tx 50 min-rx 50 multiplier 3
authentication md5 ***** key-id 8
!
```

Related Commands

命令	Description
show access-control-config	显示有关访问控制策略的摘要信息。

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。