show p - show r

- show packet tracer, on page 3
- show packet-statistics, on page 5
- show pager, on page 13
- show packet debugs, on page 14
- show parser dump, on page 16
- show password encryption, on page 17
- show path-monitoring, on page 18
- show pclu, on page 20
- show perfmon, on page 21
- show perfstats, on page 22
- show pim bsr-router, on page 23
- show pim df, on page 24
- show pim group-map, on page 25
- show pim interface, on page 26
- show pim join-prune statistic, on page 27
- show pim neighbor, on page 28
- show pim range-list, on page 29
- show pim topology, on page 30
- show pim traffic, on page 32
- show pim tunnel, on page 33
- show policy-list, on page 34
- show policy-route, on page 35
- show port-channel, on page 36
- show port-channel load-balance, on page 40
- show power inline, on page 42
- show prefix-list, on page 43
- show priority-queue, on page 45
- show processes, on page 47
- show process-tree, on page 50
- show ptp, on page 51
- show quota, on page 53
- show raid, on page 54
- show random-password, random-strong-password, on page 56

- show resource types, on page 58
- show resource usage, on page 59
- show rip database, on page 61
- show rollback-status, on page 62
- show route, on page 63
- show route-map, on page 68
- show rule hits, on page 69
- show running-config, on page 72

show packet tracer

To display information about the pcap trace output, use the **show packet tracer** command.

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

Syntax Description

packet-number	(Optional) Displays trace output for a single packet in the PCAP.
summary	(Optional) Displays PCAP summary.
detailed	(Optional) Displays trace output for all the packets in the PCAP.
status	(Optional) Displays the current execution state of the PCAP trace.
export-pcapng	(Optional) Exports the packet trace data in pcapng format.

Command Default

No default behavior or values.

Command History

Release	Modification
7.1	The command was enhanced to include output of pcap trace.

Usage Guidelines

The **show packet-tracer** command shows the packet tracer output. The **pcap trace** command allows you to display the trace buffer output of the most recently executed packet-tracer on a PCAP file.

Examples

The following is a sample output for the **show packet-tracer pcap trace summary** command:

```
> 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

Command	Description
packet tracer	Generates a 5 to 6 tuple packets against a firewall's current configurations.

show packet-statistics

To display information about non-policy related packet drops on Secure Firewall 3100, use the **show packet-statistics** command. On threat defense, run this command in the system diagnostic mode.

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

Syntax Description

interface id*slotport*	Interface name with the slot number and port number for which the statistics are displayed.
breakout	(Optional) Breakout of the port number of the ethernet.
brief	(Optional) Displays the output excluding the zero counter values.

Command Default

No default behavior or values.

Command History

Release	Modification
7.2	The command was introduced.

Usage Guidelines

The **show packet-statistics** command collates and displays packet loss data from several sources. The output helps to identify where the packets were dropped. This command consolidates the output of the following debugging commands:

- **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**

The consolidated output is in the sequence of the data path when traffic reach a device. In addition, the output is not broken or interrupted by other CLIs' output.

slot/port and **breakout***port* are used to limit the output for a specific interface. These variables and keywords are applicable only to the external switch ports and Lina interfaces. For other interfaces, these variables are ignored.

Examples

The following is sample output for the **show packet-statistics** command:

```
$ 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

To display the current page length for the CLI session, that is, the number of lines shown before the output pauses with a -- More -- indication, use the **show pager** command.

show pager

Note You cannot set the page length for the threat defense CLI.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show pager** command. Because you cannot set the page length in the threat defense CLI, the output indicates that there is no pager.

```
> show pager
no pager
```

show packet debugs

To retrieve and view the stored debug logs from the database use **show packet debugs** command. In some releases, this command might be hyphenated: **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	Matches one or more of the following options entered for filtering connection: source IP, destination IP, source port, destination port or protocol.
protocol	Name of the protocol.
source-ip	IP address of the source.
source-port	Port number of the source.
dest-ip	IP address of the destination.
dest-port	Port number of the destination.
module *module-id*	The module name to filter the debug logs.
packet-id *packet-id*	The unique packet id to filter the debug logs.
severity *0-7*	One of the following severity levels: • 0 (emergencies)—System is unusable • 1 (alert)—Immediate action is needed • 2 (critical)—Critical conditions • 3 (error)—Error conditions • 4 (warning)—Warning conditions • 5 (notice)—Normal but significant conditions • 6 (informational)—Informational messages only • 7 (debug)—Debugging messages only
time-start *time*	Returns all logs after the specified start time.
time-end *time*	Returns all logs before the specified time.

Command History

Release	Modification
6.4	This command was introduced.

Usage Guidelines

Use **show packet debugs** command to retrieve and view the stored debug logs from the database .

All keywords within [] are optional. If a particular keyword is not entered, that keyword would be considered as any. All the debugs are displayed in the ascending order of timestamp.

Examples

The following example enables TCP debugging, then shows debugging status.

```
> show packet debugs
```

Related Commands

Command	Description
debug	Enables debugging.

show parser dump

The **show parser dump** command is for internal or Cisco Technical Support use.

show password encryption

To show the password encryption configuration settings, use the **show password encryption** command.

show password encryption

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

threat defense does not allow you to configure master password encryption, so this command should always show that password encryption is Disabled and that the master key hash is not set.

If the key has been saved, “saved” appears next to the key hash. If there is no key or it has been removed from the running configuration, “Not set” appears instead of the hash value.

Examples

The following is sample output from the **show password encryption** command:

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

show path-monitoring

To display information about the path monitoring output, use the **show path monitoring** command.

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

Syntax Description

Interface*name*	Interface for which the path monitoring metric is displayed
detail	(Optional) Displays detailed information about path monitoring metrics.

Command Default

No default behavior or values.

Command History

Release	Modification
7.1	The command was introduced to display the path monitoring details for a specified interface.

Usage Guidelines

The **show path-monitoring** command shows the path monitoring output for the specified egress interface.

Examples

The following is sample output for the **show path-monitoring** command for *outside 1* interface:

```
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
```

The following is sample output for the **show path-monitoring detail** command for *outside 1* interface:

```
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

Command	Description
policy-route	Configures policy based routing on an interface.

show pclu

The **show pclu** command is for internal or Cisco Technical Support use.

show perfmon

To display information about the performance of the device, use the **show perfmon** command.

show perfmon [**detail**]

Syntax Description

detail	(Optional) Shows additional statistics. These statistics match those gathered by the Global and Per-protocol connection objects of the Cisco Unified Firewall MIB.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **perfmon** command shows performance statistics continuously at defined intervals. The **show perfmon** command allows you to display the information immediately.

Examples

The following is sample output for the **show perfmon detail** command:

```
> 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

Command	Description
perfmon	Displays detailed performance monitoring information at defined intervals.

show perfstats

To display performance statistics for the device, use the **show perfstats** command.

show perfstats

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show perfstats** command shows performance information for the Detection Engines. The command shows you a list of available engines, you pick the one whose statistics you want to view. You are then presented with a number of profiles; select the one whose content you want to view.

The files are meaningful for systems managed remotely by management center. These files typically have no content for systems managed with the local manager, device manager.

Use Crtl+C to stop the display if you decide you do not want to see the complete file. The file contents can be long.

Examples

```
> 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

To display the bootstrap router (BSR) information, use the **show pim bsr-router** command.

show pim bsr-router

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show pim bsr-router** command:

```
> 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

To display the bidirectional DF "winner" for a rendezvous point (RP) or interface, use the **show pim df** command.

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

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.
interface_name	The physical or logical interface name.
winner	(Optional) Displays the DF election winner per interface per RP.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

The following is sample output from the **show pim df** command:

```
> 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

To display group-to-protocol mapping table, use the **show pim group-map** command.

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

Syntax Description

group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table. • IPv4 or IPV6 address of the multicast group.
info-source	(Optional) Displays the group range information source.
rp-timers	(Optional) Displays uptime and expiry timers of group-to-RP mapping.

Command Default

Displays group-to-protocol mappings for all groups.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the device from different clients.

The PIM implementation on the device has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

Examples

The following is sample output form the **show pim group-map** command:

```
> 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
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.

show pim interface

To display interface-specific information for PIM, use the **show pim interface** command.

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

Syntax Description

interface_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
state-off	(Optional) Displays interfaces with PIM disabled.
state-on	(Optional) Displays interfaces with PIM enabled.

Command Default

If you do not specify an interface, PIM information for all interfaces is shown.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The threat defense device is itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

Examples

The following example displays PIM information for the inside interface:

```
> 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

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistic** command.

show pim join-prune statistic [*interface_name*]

Syntax Description

interface_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Command Default

If an interface is not specified, this command shows the join/prune statistics for all interfaces.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Clear the PIM join/prune statistics with the **clear pim counters** command.

Examples

The following is sample output from the **show pim join-prune statistic** command:

```
> 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

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

To display entries in the PIM neighbor table, use the **show pim neighbor** command.

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

Syntax Description

interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
count	(Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
detail	(Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The threat defense device is itself a PIM neighbor. Therefore, the threat defense interface is shown in the output of this command. The IP address of the threat defense device is indicated by an asterisk next to the address.

Examples

The following is sample output from the **show pim neighbor** command:

```
> 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

To display range-list information for PIM, use the **show pim range-list** command.

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

Syntax Description

config	Displays PIM CLI range list information.
rp_address	Can be either one of the following: • Name of the rendezvous point (RP), as defined in the Domain Name System (DNS) hosts table. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

Examples

The following is sample output from the **show pim range-list** command:

```
> 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

Command	Description
show pim group-map	Displays group-to-PIM mode mapping and active RP information.

show pim topology

To display PIM topology table information, use the **show pim topology** command.

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

Syntax Description

reserved	Display PIM topology table information for reserved groups.
route-count	Shows the number of routes in the PIM topology table.
detail	(Optional) Displays more detailed count information on a per-group basis.
group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table. • IPv4 or IPV6 address of the multicast group.
source	(Optional) Can be one of the following: • Name of the multicast source, as defined in the DNS hosts table. • IPv4 or IPv6 address of the multicast source.

Command Default

Topology information for all groups and sources is shown.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** command.

Examples

The following is sample output from the **show pim topology** command:

```
> 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
```

The following is sample output from the **show pim topology reserved** command:

```
> 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
```

The following is sample output from the **show pim topology route-count** command:

```
> 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

Command	Description
show mrib route	Displays the MRIB table.

show pim traffic

To display PIM traffic counters, use the **show pim traffic** command.

show pim traffic

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Clear the PIM traffic counters with the **clear pim counters** command.

Examples

The following is sample output from the **show pim traffic** command:

```
> 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

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

To display information about the PIM tunnel interfaces, use the **show pim tunnel** command.

show pim tunnel [*interface_name*]

Syntax Description

interface_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Command Default

If an interface is not specified, this command shows the PIM tunnel information for all interfaces.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the rendezvous point (RP). On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

Examples

The following is sample output from the **show pim tunnel** command:

```
> 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

Command	Description
show pim topology	Displays the PIM topology table.

show policy-list

To display information about a configured policy list and policy list entries, use the **show policy-list** command.

show policy-list [*policy_list_name*]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Policy lists are used in BGP routing as matching criteria for route maps.

Examples

The following is sample output from the **show policy-list** command:

```
> 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

To show policy-based routing configurations, use the **show policy-route** command.

show policy-route

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show policy-route** command:

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

show port-channel

To display EtherChannel information in a detailed and one-line summary form or to display the port and port-channel information, use the **show port-channel** command.

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

Syntax Description

brief	(Default) Shows a brief display.
channel_group_number	(Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
detail	(Optional) Shows a detailed display.
port	(Optional) Shows information for each interface.
protocol	(Optional) Shows the EtherChannel protocol, such as LACP if enabled.
summary	(Optional) Shows a summary of port-channels.

Command Default

The default is **brief**.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show port-channel** command:

```
> 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
```

The following is sample output from the **show port-channel summary** command:

```
> 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
```

The following is sample output from the **show port-channel detail** command:

```
> 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
```

The following is sample output from the **show port-channel port** command:

```
> 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
```

The following is sample output from the **show port-channel protocol** command:

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

Related Commands

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier, and neighbor details.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

show port-channel load-balance

For EtherChannels, to display the current port-channel load-balance algorithm, and optionally to view the member interface selected for a given set of parameters, use the **show port-channel load-balance** command.

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

Syntax Description

channel_group_number	Specifies the EtherChannel channel group number, between 1 and 48.
hash-result	(Optional) Shows the member interface chosen after hashing values you enter for the current load-balancing algorithm.
ip	(Optional) Specifies IPv4 packet parameters.
ipv6	(Optional) Specifies IPv6 packet parameters.
l4port	(Optional) Specifies port packet parameters.
mac	(Optional) Specifies MAC addresss packet parameters.
mixed	(Optional) Specifies a combination of IP or IPv6 parameters, along with ports and/or the VLAN ID.
parameters	(Optional) Packet parameters, depending on the type. For example, for ip, you can specify the source IP address, the destination IP address, and/or the VLAN ID.
vlan-only *number*	(Optional) Specifies the VLAN ID for a packet, from 0-4095.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

By default, the device balances the packet load on interfaces according to the source and destination IP address (**src-dst-ip**) of the packet.

This command lets you view the current load-balancing algorithm, but, with the **hash-result** keyword, also lets you test which member interface will be chosen for a packet with given parameters. This command only tests against the current load-balancing algorithm. For example, if the algorithm is src-dst-ip, then enter the IPv4 or IPv6 source and destination IP addresses. If you enter other arguments not used by the current algorithm, they are ignored, and the unentered values actually used by the algorithm default to 0. For example, if the algorithm is vlan-src-ip, then enter:

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

If you enter the following, then the vlan-src-ip algorithm assumes a source IP address of 0.0.0.0 and VLAN 0, and ignores the values you enter:

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

Examples

The following is sample output from the **show port-channel 1 load-balance** command:

```
> 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
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters match the current algorithm (src-dst-ip):

```
> 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
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters do not match the current algorithm (src-dst-ip), and the hash uses 0 values:

```
> 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

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.

show power inline

For models with PoE interfaces, use the **show power inline** command to show power status of the interfaces.

Note Supported for the Firepower 1010 only.

show power inline

Command History

Release	Modification
6.5	This command was introduced.

Usage Guidelines

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+.

Examples

The following is sample output from the **show power inline** command for the Firepower 1010:.

```
> 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
```

The following table shows each field description:

Table 1: show power inline Fields

Field	Description
Interface	Shows all interfaces on the threat defense, including ones that do not have PoE available.
Power	Shows whether the power is On or Off. If a device does not need power, if there is no device on that interface, or if the interface is shut down the value is Off. If the interface does not support PoE, then the value is n/a.
Class	Shows the PoE class of the connected device.
Current (mA)	Shows the current being used.
Voltage (V)	Shows the voltage being used.

show prefix-list

To list prefix lists that are configured to match IPv4 traffic, use the **show prefix-list** command.

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

Syntax Description

detail	Show details about prefix lists.
summary	Show a summary of prefix lists.
prefix_list_name	Name of a prefix list.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits). The length of the network mask can be from 0 to 32. You can optionally include one of the following keywords: • **longer** displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match** displays the first entry of the specified prefix list that matches the given network/length.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show prefix-list** command with a prefix-list named “test.”

```
> 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

Command	Description
clear prefix-list	Reset the hit count on an IP prefix list.
show bgp prefix-list	Displays information about a prefix list or prefix list entries in the context of Border Gateway Protocol.

Command	Description
show ipv6 prefix-list	Displays information about IPv6 prefix lists.

show priority-queue

To display the priority-queue configuration or statistics for an interface, use the **show priority-queue** command.

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

Syntax Description

config	Show the queue and TX-ring limits for the interface priority queues.
interface_name	(Optional) Specifies the name of the interface for which you want to show the configuration or the best-effort and low-latency queue statistical details.
statistics	Show the best-effort and low-latency queue statistical details.

Command History

Release	Modification
6.3	This command was introduced.

Examples

This example shows statistics for the interface named test. In the output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
> 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
```

The following example shows the configuration of the priority queues on all configured interfaces.

```
> 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
```

Command	Description
clear priority-queue statistics	Resets priority queue statistics to zero.

show processes

To display a list of the processes that are running on the device, use the **show processes** command.

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

Syntax Description

cpu-hog	Shows number and detail of processes that are hogging the CPU (that is, using the CPU for more than 100 milliseconds).
cpu-usage	Shows percentage of CPU used by each process for the last 5 seconds, 1 minute and 5 minutes.
internals	Shows internal details of each process.
memory	Shows memory allocation for each process.
non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes.
system	(Optional) Shows information about the processes currently running on the system.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Processes are lightweight threads that require only a few instructions. The **show processes** commands display a list of the processes that are running on the device, as follows:

Command	Data Displayed	Description
show processes	PC	Program counter.
show processes	SP	Stack pointer.
show processes	STATE	Address of thread queue.
show processes	Runtime	Number of milliseconds that the thread has been running based on CPU clock cycles. The accurracy is within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (<10ns resolution) instead of clock ticks (10ms resolution).
show processes	SBASE	Stack base address.
show processes	Stack	Current number of bytes in use and the total size of the stack.
show processes	Process	Function of the thread.
show processes cpu-usage	MAXHOG	Maximum CPU hog runtime in milliseconds.

Command	Data Displayed	Description
show processes cpu-usage	NUMHOG	Number of CPU hog runs.
show processes cpu-usage	LASTHOG	Last CPU hog runtime in milliseconds.
show processes cpu-usage	PC	Instruction pointer of the CPU hogging process.
show processes cpu-usage	Traceback	Stack trace of the CPU hogging process. The traceback can have up to 14 addresses.
show processes internals	Invoked Calls	Number of times the scheduler ran the process.
show processes internals	Giveups	Number of times the process yielded the CPU back to the scheduler.

Use the **show processes cpu-usage** command to narrow down a particular process on the device that might be using the CPU. You can use the **sorted** and **non-zero** commands to further customize the output of the **show processes cpu-usage** command.

With the scheduler and total summary lines, you can run two consecutive **show proccesses** commands and compare the output to determine:

- Consumption of 100% of the CPU.
- Percentage of CPU used by each thread, determined by comparing the runtime delta of a thread to the total runtime delta.

The device runs as a single process with many different threads of execution. The output of this command actually shows memory allocations and free memory on a per-thread basis. Because these threads work in cooperation on data flows and other operations pertinent to operation of the device, one thread may allocate a block of memory while a different thread may free it. The last row of output contains the total counts over all threads. Only this row may be used to track potential memory leaks by monitoring the difference between allocations and free memory.

Examples

The following example shows how to display a list of processes that are running. Command output wraps.

```
> 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
```

The following example shows how to list system processes.

```
> 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...)
```

The following example shows how to display the percentage of CPU used by each process:

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

The following examples show how to display the number and detail of processes that are hogging the CPU:

```
> 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...)
```

The following example shows how to display the memory allocation for each process:

```
> 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...)
```

The following example shows how to display the internal details of each process:

```
> 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

To display the system processes in a tree relationship, use the **show process-tree** command.

show process-tree

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The output for this command is mainly of interest to Cisco Technical Support.

Examples

The following is an example of showing the process tree.

```
> 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

To display Precision Time Protocol (PTP) statistics and clock information, use the **show ptp** command.

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

Syntax Description

clock	Displays PTP clock properties.
port [*interface_name*]	Displays PTP port information for the interfaces. You can optionally specify an interface name to see information about that interface only.

Command History

Release	Modification
6.5	This command was introduced.

Example

The following example shows that PTP is not configured. PTP packets can pass through the device, but the device does not use the PTP clocks.

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

The following example shows PTP clock properties:

```
> 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
```

The following example shows PTP port information for all PTP-enabled interfaces:

```
> 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

To show quota statistics for the current session, use the **show quota** command.

show quota [**management-session**]

Syntax Description

management-session	Shows statistics for the current management session.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You cannot configure management session quotas as threat defense. This command should always show no limits.

Examples

The following example shows quota statistics.

```
> 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

To view the status of SSDs in the RAID, use the **show raid** command.

Note This command is only supported on the Secure Firewall 3100.

show raid

Command History

Release	Modification
7.1	This command was introduced.

Examples

The following sample display shows two SSDs in the RAID:

```
> 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:
```

The following sample display shows one SSD in the RAID; disk2 is not present, and the RAID is shown as "degraded:"

```
> 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

Command	Description
configure raid	Adds or removes an SSD from the RAID.
show ssd	Shows SSD status.

show random-password, random-strong-password

To generate a password that you can use when changing your password, use one of the following commands

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

Syntax Description

random-password	Generates a random password that does not include special characters.
random-strong-password	Generates a strong random password, that is, one that includes special characters.
length	Specifies the length of the password to be generated, 8-127 characters.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Generating passwords works on FXOS platforms only. You can use these commands in conjunction with changing your password, if you do not want to come up with your own password.

After you enter the command, a random password is shown. You can copy/paste or make a note of the password. On the next keystroke of any kind, the password is wiped from the output so that it cannot be scraped by another user.

Example

The following example shows how to change the password for joeuser using a generated password. First, use **show user** to determine the minimum password length and whether a strong password is required. In this case, the minimum length (MinL) is 8 characters, and password strength (Str) is Enabled. Next, we generate a strong password of 12 characters (exceeding the minimum length). Copy this to the clipboard, then paste it into the change password command, either **configure user password** when changing another user's password, or **configure password** when changing the password for the account you are logged into.

```
> 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>
```

The following example shows what you see if you try to generate a password on a non-FXOS platform, or on an FXOS platform whose FXOS version does not support random password generation.

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

Command	Description
configure password	Sets the password for the logged-in user.
configure user minpasswdlength	Adds a new user.
configure user password	Sets password for specified user.
configure user strength-check	Sets strong password requirements.
show user	Shows user accounts.

show resource types

To view the resource types for which the device tracks usage, use the **show resource types** command.

show resource types

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following sample display shows the resource types:

```
> 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

Command	Description
clear resource usage	Clears the resource usage statistics
show resource usage	Shows the resource usage of the device.

show resource usage

To view the resource usage of the device, use the **show resource usage** command.

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

Syntax Description

all	All types.
count_threshold	Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify all for the counter name, then the count threshold applies to the current usage. To show all resources, set the count threshold to 0.
counter *counter_name*	Shows counts for the following counter types: • **current**—Shows the active concurrent instances or the current rate of the resource. • **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted. • **denied**—Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column. • **all**—(Default) Shows all statistics.
detail	Shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.
resource {[**rate**] *resource_name* | **all**}	Shows the usage of a specific resource. Specify **all** for all resources. Specify rate to show the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The **conns** resource is also measured as concurrent connections; only use the rate keyword to view the connections per second. See the Usage Guidelines section for a list of resource names.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

When you use the **resource** keyword, resources include the following types:

- **asdm**—The feature related to this keyword is not supported by threat defense.
- **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
- **hosts**—Hosts that can connect through the threat defense device.
- **ipsec**—IPSec management tunnels

- **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
- **rate**—Rate-measured resources. Specify **conns**, **inspects**, or **syslogs**.
- **routes**—Routing Table entries.
- **ssh**—SSH sessions.
- **storage**—Storage Limit Size, in MB.
- **telnet**—Telnet sessions.
- **vpn** —VPN resources.
- **vpn anyconnect**—AnyConnect Premium license limit.
- **vpn ikev1 in-negotiation**—Number of IKEv1 sessions which can be in negotiation.
- **VPN Other**—Site-to-site VPN sessions.
- **VPN Burst Other**—Site-to-site VPN burst sessions.
- **xlates**—NAT translations.

Examples

The following is sample output from the **show resource usage** command, which shows the resource usage for all resources. The device is in single context mode, so the context is shown as System.

```
> 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

Command	Description
clear resource usage	Clears the resource usage statistics
show resource types	Shows a list of resource types.

show rip database

To display the information that is stored in the RIP topological database, use the **show rip database** command.

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

Syntax Description

ip_addr	(Optional) Limits the display routes for the specified network address.
mask	(Optional) Specifies the network mask for the optional network address.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The RIP database contains all of the routes learned through RIP. Routes that appear in this database may not necessarily appear in the routing table.

Examples

The following is sample output from the **show rip database** command:

```
> 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
```

The following is sample output from the **show rip database** command with a network address and mask:

```
> 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

To show the status of the latest rollback job (if any) sent from management center, use the **show rollback-status** command.

show rollback-status

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

If management center needs to roll back configuration changes during a deployment job, it sends a request to the device and then the management connection from management center to the device is reset. You can use this command to see the status of the rollback job.

The rollback job relates to the commands configured in the running configuration file only; it does not roll back the Snort configuration.

If the device is running in high availability mode, use this command on the active unit only. In a cluster, use the command on the master unit only.

The information includes the following:

- **Status**—The status of the most recent rollback job.
  - None—No rollback job has been ever requested.
  - In Progress—The system has received the rollback request, and the rollback job is in progress.
  - Succeeded—The rollback has completed successfully.
  - Reverted—Rollback to the configuration sent from device manager failed. The system reverts to the last saved configuration.
  - Failed—Rollback completed with error.
- Start Time/End Time—The starting and ending times for the job. N/A means there was no job; for end time, N/A can also mean that the job is still in progress.

Examples

The following example shows the normal situation, where no rollback job has ever been requested.

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

Related Commands

Command	Description
show running-config	Shows the configuration that is defined in the running configuration file.

show route

To display the routing table for the data interfaces, use the **show route** command.

The parameters you can use with this command differ depending on the firewall mode of the device, routed or transparent. This is indicated in the syntax description.

show route [**vrf** *name* | **all**] **summary** [**management-only**] [**cluster** | **failover** | *hostname* | *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*	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number) for the BGP route. The AS number limits the display to route entries that use the specified AS number.
cluster	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number).
connected	(Routed, transparent.) Displays connected routes.
eigrp *process_id*	(Routed.) Displays EIGRP routes. threat defense does not support EIGRP, however.
failover	(Routed.) Displays the current sequence number of the routing table and routing entries after failover has occurred, and a standby unit becomes the active unit.
hostname	(Routed, transparent.) Displays routes to the specified destination hostname. You must configure DNS for hostname resolution to work.
interface_name	(Routed, transparent.) Displays route entries that use the specified interface.
ip_address mask	(Routed, transparent.) Displays routes to the specified destination.
isis	(Routed.) Displays IS-IS routes.
longer-prefixes	(Routed, transparent.) Displays routes that match the specified ip_address/mask pair only
management-only	(Routed, transparent.) Displays routes in the IPv4 management routing table.
ospf *process_id*	(Routed.) Displays OSPF routes.
rip	(Routed.) Displays RIP routes.
static	(Routed, transparent.) Displays static routes.
summary	(Routed, transparent.) Displays the current state of the routing table.

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

Command History

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

Usage Guidelines

The **show route** command provides output similar to the **show ipv6 route** command, except that the information is IPv4-specific. The routes shown are for the data interfaces only, not for the virtual management interface. To see the default gateway for the management interface, use the **show network** command. To see routes on the management interface, use the **show network-static-routes** command.

Note The **clustering** and **failover** keywords do not appear unless these features are configured on the threat defense device.

The **show route** command lists the "best" routes for new connections. When you send a permitted TCP SYN to the backup interface, the threat defense device can only respond using the same interface. If there is no default route in the RIB on that interface, the device drops the packet because of no adjacency. Everything that is configured as shown in the **show running-config route** command is maintained in certain data structures in the system.

You can check the backend interface-specific routing table with the **show asp table routing** command. This design is similar to OSPF or EIGRP, in which the protocol-specific route database is not the same as the global routing table, which only displays the "best" routes. This behavior is by design.

Examples

The following is sample output from the **show route** command:

```
> 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
```

The following is sample output of the **show route failover** command, which shows the synchronization of OSPF and EIGRP routes to the standby unit after failover:

```
> 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
```

The following is sample output from the **show route cluster** command:

```
> 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
```

The following is sample output from the **show route summary** command:

```
> 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
```

The following example displays routes in all virtual routers when you have enabled virtual routing and forwarding (VRF). In this example, there are two virtual routers (test1 and test2) in addition to the global router, which is shown first.

```
> 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
```

The following example displays routes for the virtual router named red. Note that static routes leaked to other virtual routers are indicated with the key SI.

```
> 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
```

The following example displays summary of routes for all VRFs.

```
> 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

Command	Description
show ipv6 route	Shows the IPv6 routing table.
show vrf	Shows the virtual routers defined on the system.

show route-map

To show route map information, use the **show route-map** command.

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

Syntax Description

all	Show information about both static and dynamic route maps.
dynamic	Show only information about dynamic route maps.
application *application*	Application that created the route map.
route_map	Name of the route map.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show route-map dynamic** command:

```
> 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

To display rule hit information for all evaluated rules of access control policies and prefilter policies, use the **show rule hits** command.

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

Syntax Description

cumulative	(Optional.) Show the cumulative sum of rule hits in all cluster or high-availability (HA) nodes. Hit count is calculated per node, so the sum shows the total hits across the cluster or HA pair.
id*number*	(Optional) The ID of a rule. Including this argument limits the displayed information to the specified rule. You cannot specify any other options when you specify the ID. Use the **show access-list** command to identify a rule ID.
node-wise	(Optional.) Show the current hit count for each unit in the cluster or HA pair.
raw	(Optional) Displays the rule hit information in .csv format.
gt *#hit-count*	(Optional) Displays all the rules that have a hit count greater than *#hit-count*.
lt *#hit-count*	(Optional) Displays all the rules that have a hit count lesser than *#hit-count*.
range *#hit-count1 #hit-count2*	(Optional) Displays all the rules that have a hit count in-between *#hit-count1* and *#hit-count2*.

Command Default

If you do not specify a rule ID, the rule hit information for all the rules are shown.

Command History

Release	Modification
6.4	This command was introduced.
7.2	The **cumulative** and **node-wise** keywords were added.

Usage Guidelines

The rule hit information covers only the access control rules and prefilter rules.

You can more easily see rule hit information using the local or remote device managers when viewing an access control or prefilter policy. Note that the rule hit information shown in this command is based on the real rule, and not on any access control entry (ACE) in any ACL that was generated to partially implement the rule. Thus, hit count information shown by this command is not equivalent to hit counts displayed by the **show access-list** command.

Use the **show access-list** command to identify a rule ID. However, not all the rules are listed in the output of this command. For management center-managed devices, you can use a REST API GET operation on the following URLs to see all the rules and their IDs:

- `/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`

Examples

The following example displays rule hit information:

```
> 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
```

The following example shows the summary hit count across all units in a cluster or HA pair.

```
> 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
```

The following example shows the hit count for each unit in a cluster or HA pair. The hit counts are kept separately for each device.

```
> 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

Command	Description
clear rule hits	Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.
show cluster rule hits	Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.

Command	Description
cluster exec show rule hits	Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.
cluster exec clear rule hits	Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.

show running-config

To display the configuration that is currently running on the device, use the **show running-config** command.

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

Syntax Description

all	Displays the entire operating configuration, including defaults.
command	Displays the configuration associated with a specific command. For available commands, see the CLI help using **show running-config ?**. **Note** threat defense does not directly support every command listed in the CLI help. There might not be any configuration for a given option. Some options can be configured only using a FlexConfig from management center.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show running-config** command displays the active configuration in memory (including saved configuration changes) on the device. You cannot directly configure these commands. Instead, they are configured by the manager controlling the device, for example, management center or device manager.

However, this is a partial configuration. It shows what can be configured using ASA Software configuration commands only, although some commands might be specific to threat defense. These commands are ported to threat defense. Thus, you should use the information in the running configuration as a troubleshooting aid only. Use the management centerdevice manager as the main means to analyze the device configuration.

Examples

The following is sample output from the **show running-config** command:

```
> 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
>
```

To view the BFD global configuration settings, use output modifiers to filter the BFD related configuration. The following is sample output from the **show running-config bfd** command using the output modifiers:

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

The following is sample output from the **show running-config bfd-template** command using the output modifiers:

```
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
!
```

To view the default configuration difference between Snort 2 and Snort 3, use output modifiers to filter the Snort 2 and Snort 3 dp-tcp-proxy information.

Attention By default, the dp-tcp-proxy command is enabled on Snort 2 and disabled on Snort 3.

- For Snort 2, the dp-tcp-proxy command is enabled because SSL inspection is part of deep packet inspection (DAQ).
- For Snort 3, the dp-tcp-proxy command is pushed to the firewall engine in case either the SSL policy is attached with the access control policy or certificate-visibility is enabled under access control policy.

The following is sample output from the **show running-config all | include dp-tcp-proxy** command using the output modifiers:

```
ciscoftd# show running-config all | include dp-tcp-proxy
no dp-tcp-proxy  >> This command is disabled on Snort 3
```

Related Commands

Command	Description
show access-control-config	Shows summary information about the access control policy.