

Chapter 7

Firewall Filters Operational Mode Commands

Table 13 summarizes the command-line interface (CLI) commands you can use to monitor firewall filters. In the table, the commands are grouped by functionality. In the remainder of this chapter, they are explained alphabetically.

Table 13: Commands for Monitoring and Managing Firewall Filters

Task or Information to Monitor	Command
Counters for firewall filters	show firewall filter on page 228
Clear firewall filter counters	clear firewall on page 227
Firewall filter log information	show firewall log on page 229
Counters for policers	show policer on page 230

clear firewall

Syntax	clear firewall (all counter <i>counter-name</i> filter <i>filter-name</i>)
Description	Clear statistics about configured firewall filters.
Options	all—Clear the packet and byte counts for all filters. counter <i>counter-name</i> —Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action. filter <i>filter-name</i> —Clear the packet and byte counts for the specified firewall filter.
Required Privilege Level	clear

show firewall filter

Syntax	show firewall filter <i>filter-name</i>
Description	Display statistics about configured firewall filters.
Options	<i>filter-name</i> —Display information about a specific filter.
Required Privilege Level	view
Output Fields	<p>Filter—Name of a filter that has been configured with the filter statement at the [edit firewall] hierarchy level. When an interface-specific filter is used, the name of the filter is followed by the full interface name and by either -i for an input filter, or -o for an output filter.</p> <p>Counters—Display filter counter information.</p> <p>Name—Name of a filter counter that has been configured with the counter firewall filter action.</p> <p>Bytes—Number of bytes that match the filter term under which the counter action is specified.</p> <p>Packets—Number of packets that matched the filter term under which the counter action is specified.</p> <p>Policers—Display policer information.</p> <p>Name—Name of policer.</p> <p>Packets—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-spec packet counts, not all packets policed by the policer.</p>

Sample Output

```

user@host> show firewall filter
Filter: accept_inet6
Counters:
Name          Bytes    Packets
accept        0        0

Filter: test
Counters:
Name          Bytes    Packets
Counter-1    0        0
Counter-2    0        0
Policers:
Name          Packets
Policer-1    0
Filter: input_filter

Filter: ftf_filter
Counters:
Name          Bytes    Packets
ftf          297920   4655
Filter: vrf_filter
Counters:
Name          Bytes    Packets
vrf          0        0

```

show firewall log

Syntax	show firewall log <interface <i>interface-name</i> > <detail>
Description	Display log information about firewall filters.
Options	<p>detail—(Optional) Display detailed information.</p> <p>interface <i>interface-name</i>—(Optional) Display log information about a specific interface.</p>
Required Privilege Level	view
Output Fields	<p>Time—Time that the event occurred.</p> <p>Filter—Name of a filter that has been configured with the filter statement at the [edit firewall] hierarchy level.</p> <p>A hyphen (-) indicates that the packet was handled by the Packet Forwarding Engine.</p> <p>A space (no hyphen) indicates the packet was handled by the Routing Engine.</p> <p>The notation pfe indicates packets logged by the Packet Forwarding Engine hardware filters.</p> <p>Act—Filter action:</p> <p>A—Accept</p> <p>D—Discard</p> <p>R—Reject</p> <p>Interface—Ingress interface for the packet.</p> <p>Pro—Packet's protocol name or number: egp, gre, icmp, ipip, ospf, pim, rsvp, tcp, or udp.</p> <p>Source address—Packet's source address.</p> <p>Destination address—Packet's destination address and port.</p>

Sample Output user@host> **show firewall log**

```

Time   Filter Act Interface   Pro Source address Destination address
16:08:04 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:24373
16:08:03 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:29531
16:08:02 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:27265
16:08:01 pfe      A so-1/1/0.0   OSP 123.168.10.65 212.0.0.5:48
16:08:01 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:43943
16:08:00 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:58572
16:07:59 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:56307
16:07:58 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:60185
16:07:57 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:1600
16:07:56 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:6502
16:07:55 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:17548
16:07:54 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:5298
16:07:53 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:24536
16:07:52 sample-test A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:24373
16:07:52 sample-test A local          ICM 123.168.10.66 123.168.10.65:22325
16:07:52 pfe      A so-1/1/0.0   ICM 123.168.10.65 123.168.10.66:27900
...

```

show policer

Syntax show policer <*policer-name*>

Description Display number of policed packets for a given policer. If no policer is specified, the policed packets for all policers is displayed.

Options *policer-name*—(Optional) Display the number of policed packets for a particular policer.

Required Privilege Level view

Output Fields Policer name—Name of the policer.

Packets—Total number of packets policed by the specified policer.

Sample Output user@host> **show policer**

```

Policers:
Name                               Packets
__default_arp_policer__            0
fe-1/2/0.0-out-policer             3496661237
fe-1/2/1.0-out-policer             3432710964

```