Configuring Firewall Filters (CLI Procedure)

You configure firewall filters on EX-series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

Configuring a Firewall Filter

To configure a firewall filter:

1. Configure the family address type for the firewall filter:
   - For a firewall filter that is applied to a port or VLAN, specify the family address type ethernet-switching (or bridge) to filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets, for example:

     ```
     [edit firewall]
     user@switch# set family ethernet-switching
     ```

   - For a firewall filter that is applied to a Layer 3 (routed) interface, specify the family address type inet to filter IPv4 packets, for example:

     ```
     [edit firewall]
     user@switch# set family inet
     ```

2. Specify the filter name:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter ingress-port-filter
   ```

   The filter name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. Each filter name must be unique.

3. If you want to apply a firewall filter to multiple interfaces and name individual firewall counters specific to each interface, configure the interface-specific option:

   ```
   [edit firewall family ethernet-switching filter ingress-port-filter]
   user@switch# set interface-specific
   ```

4. Specify a term name:

   ```
   [edit firewall family ethernet-switching filter ingress-port-filter]
   ```

```
user@switch# set term term-one
```

The term name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long.

A firewall filter can contain one or more terms. Each term name must be unique within a filter.

NOTE: For EX-series switches, the number of terms allowed per firewall filter cannot exceed 2048. If you attempt to configure a firewall filter that exceeds this limit, the switch returns the following message after the commit operation:

```
Number of filter terms 2048 exceeded: Only 2048 terms can be defined.
```

5. In each firewall filter term, specify the match conditions to use to match components of a packet.

   To specify match conditions to match on packets that contain a specific source-address and source-port—for example:

   ```
   [edit firewall family ethernet-switching filter ingress-port-filter term
   term-one]
   user@switch# set from source-address 192.0.2.14
   user@switch# set from source-port 80
   ```

   You can specify one or more match conditions in a single from statement. For a match to occur, the packet must match all the conditions in the term.

   The from statement is optional, but if included in a term, the from statement cannot be empty. If you omit the from statement, all packets are considered to match.

6. In each firewall filter term, specify the actions to take if the packet matches all the conditions in that term.

   You can specify an action and/or action modifiers:

   - To specify a filter action, for example, to discard packets that match the conditions of the filter term:

     ```
     [edit firewall family ethernet-switching filter ingress-port-filter term
     term-one]
     user@switch# set then discard
     ```

     You can specify no more than one action (accept, discard, or routing-instance) per filter term.

   - To specify action modifiers, for example, to count and classify packets in a forwarding class:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one]
user@switch# set then count counter-one
user@switch# set then forwarding-class expedited-forwarding
```

You can specify any of the following action modifiers in a then statement:

- analyzer *analyzer-name*—Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. An analyzer must be configured under the ethernet-switching family address type. See Configuring Port Mirroring to Analyze Traffic (CLI Procedure).
- count *counter-name*—Count the number of packets that pass this filter term.

NOTE: We recommend that you configure a counter for each term in a firewall filter, so that you can monitor the number of packets that match the conditions specified in each filter term.

- forwarding-class *class*—Classify packets in a forwarding class.
- loss-priority *priority*—Set the priority of dropping a packet.
- policer *policer-name*—Apply rate-limiting to the traffic.

If you omit the then statement or do not specify an action, packets that match all the conditions in the from statement are accepted. However, you should always explicitly configure an action and/or action modifier in the then statement. You can include no more than one action statement, but you can use any combination of action modifiers. For an action or action modifier to take effect, all conditions in the from statement must match.

NOTE: Implicit discard is also applicable to a firewall filter applied to the loopback interface, lo0.

Applying a Firewall Filter to a Port on a Switch

To apply a firewall filter to an ingress port on a switch:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set ge-0/0/1 description "filter to limit tcp traffic filter
at trunk port for employee-vlan and voice-vlan"
```

2. Specify the unit number and family address type for the interface:

```
[edit interfaces]
user@switch# set ge-0/0/1 unit 0 family ethernet-switching
ethernet-switching
```

For firewall filters that are applied to ports, the family address type must be ethernet-switching (or bridge).

3. To apply a firewall filter to filter packets that are entering a port:

```
[edit interfaces]
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input
ingress-port-filter
```

You cannot apply a firewall filter to filter packets that are exiting ports.

NOTE: You can apply no more than one firewall filter per ingress port.

Applying a Firewall Filter to a VLAN on a Network

To apply a firewall filter to a VLAN:

1. Specify the VLAN name and VLAN ID and provide a meaningful description of the firewall filter and the VLAN to which the filter is applied:

```
[edit vlans]
user@switch# set employee-vlan vlan 20 vlan-description "filter to rate
limit traffic on employee-vlan"
```

2. Apply firewall filters to filter packets that are entering or exiting the VLAN:
   - To apply a firewall filter to filter packets that are entering the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan 20 filter input ingress-vlan-filter
```

   - To apply a firewall filter to filter packets that are exiting the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan 20 filter output egress-vlan-filter
```

NOTE: You can apply no more than one firewall filter per VLAN, per direction.

Applying a Firewall Filter to a Layer 3 (Routed) Interface

To apply a firewall filter to a Layer 3 routed interface on a switch:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set ge-0/1/0 description "filter to count and monitor
employee-vlan traffic on layer 3 interface"
```

2. Specify the unit number, family address type, and address for the interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family ethernet-switching inet
source-address 10.10.10.1/24
```

   For firewall filters applied to Layer 3 routed interfaces, the family address type must be inet.

3. You can apply firewall filters to filter packets that are entering or exiting a Layer 3 routed interface:

   - To apply a firewall filter to filter packets that are entering a Layer 3 interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet source-address 10.10.10.1/24
filter input ingress-router-filter
```

   - To apply a firewall filter to filter packets that are exiting a Layer 3 interface, include the filter input statement, for example:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet source-address 10.10.10.1/24
filter output egress-router-filter
```

NOTE: You can apply no more than one firewall filter per Layer 3 interface, per direction.

Related Topics

- Configuring Firewall Filters (J-Web Procedure)
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX-series Switches
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX-series Switches
- Verifying That Firewall Filters Are Operational
- Monitoring Firewall Filter Traffic

- Configuring Policers to Control Traffic Rates (CLI Procedure)
- Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior (CLI Procedure)
- Firewall Filter Match Conditions and Actions for EX-series Switches
- Firewall Filters for EX-series Switches Overview