## Configuring Firewall Filters (J-Web Procedure)

To configure firewall filters settings using the J-Web interface:

1. Select Configure > Security > Filters.

   The Firewall Filter Configuration screen displays a list of all configured VLAN or router filters and the ports or VLANs associated with a particular filter.

2. Click one:

   - Add—Select this option to create a new filter. Enter information as specified in Table 1.
   - Edit—Select this option to edit an existing filter settings. Enter information as specified in Table 1.
   - Delete—Select this option to delete a filter.
   - Term Up—Select this option to move a term up in the filter term list.
   - Term Down—Select this option to move a term down in the filter term list.

**Table 1: Create a New Filter**

| Field | Function | Your Action |
|---|---|---|
| **Filter tab** | | |
| Filter type | Specifies the filter type: Port/VLAN firewall filter or Router firewall filter. | Select the filter type. |
| Filter name | Specifies the name for the filter. | Enter a name. |
| Select terms to be part of the filter | Specifies the terms to be associated with the filter. Add new terms or edit existing terms. | Click Add to add new terms. Enter information as specified in Table 2. |
| **Association tab** | | |
| Port Associations | Specifies the ports with which the filter is associated.<br>**NOTE:** For a Port/VLAN filter type only Ingress direction is supported for port association. | 1. Click Add.<br>2. Select the direction: Ingress or Egress.<br>3. Select the ports.<br>4. Click OK. |
| VLAN Associations | Specifies the VLANs with which the filter is associated.<br>**NOTE:** Because Router firewall filters can be associated with ports only, this section is not displayed for a Router firewall filter. | 1. Click Add.<br>2. Select the direction: Ingress or Egress.<br>3. Select the VLANs.<br>4. Click OK. |

**Table 2: Create a New Term**

| Field | Function | Your Action |
|---|---|---|
| Term Name | Specifies the name of the term. | Enter a name. |
| Protocols | Specifies the protocols to be associated with the term. | 1. Click Add.<br>2. Select the protocols.<br>3. Click OK. |
| Source/Destination | Specifies the IP address, MAC address, and available ports.<br><br>**NOTE:** MAC address is specified only for a Port/VLAN filters. | Click Edit to enter the IP address and select the ports for the source and destination. |
| Action | Specifies the packet actions for the term. | Select one:<br>■ Accept<br>■ Discard |
| More | Specifies advanced configuration options for the filter. | Select the Match conditions as specified in Table 3.<br><br>Select the packet actions for the term as specified in Table 3. |

**Table 3: Term-Advanced Options**

| Table | Function | Your Action |
|---|---|---|
| ICMP Type | Specifies the ICMP packet type field. Typically, you specify this match in conjunction with the protocol match to determine which protocol is being used on the port. | Select the option from the list. |
| ICMP Code | Specifies more specific information than icmp-type. Because the value's meaning depends upon the associated icmp-type, you must specify icmp-type along with icmp-code. The keywords are grouped by the ICMP type with which they are associated. | Select one:<br>■ Parameter-problem<br>■ Redirect<br>■ Time-exceeded<br>■ Unreachable |
| Fragment Flags | Specifies the IP fragmentation flags.<br><br>**NOTE:** Fragment flags is supported on ingress ports, VLANs, and router interfaces. | Select either the option is-fragement or enter a combination of fragment flags. |
| TCP Flags | Specifies one or more TCP flags.<br><br>**NOTE:** TCP flags is supported on ingress ports, VLANs, and router interfaces. | Select either the option tcp-initial or enter a combination of TCP flags. |

**Table 3: Term-Advanced Options** *(continued)*

| Table | Function | Your Action |
|---|---|---|
| IP Precedence | Specifies IP precedence. The options are: assured forwarding, best-effort, expedited-forwarding, network-control.<br><br>**NOTE:** IP precedence and DSCP number cannot be specified together for the same term. | Select the option from the list. |
| Interface | Specifies the interface association. | Select the interface from the list. |
| Ether Type | Specifies the ethernet type field of a packet.<br><br>**NOTE:** This option is not applicable for a Routing filter. | Select one:<br>■ Arp<br>■ Dot 1q |
| dot1q-tag | Specifies the tag field in the Ethernet header. Values can be from 1 through 4095.<br><br>**NOTE:** This option is not applicable for a Routing filter. | Enter the required number. |
| Dot 1q User Priority | Specifies the user-priority field of the tagged Ethernet packet. User-priority values can be 0–7.<br><br>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed)<br>■ background (1)—Background<br>■ best-effort (0)—Best effort<br>■ controlled-load (4)—Controlled load<br>■ excellent-load (3)—Excellent load<br>■ network-control (7)—Network control reserved traffic<br>■ standard (2)—Standard or Spare<br>■ video (5)—Video<br>■ voice (6)—Voice<br><br>**NOTE:** This option is not applicable for a Routing filter. | Enter a number or the corresponding text synonym. |
| DSCP Number | Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP. | Select the DSCP number from the list. |
| Select VLAN | Specifies the VLAN to be associated.<br><br>**NOTE:** This option is not applicable for a Routing filter. | Select the VLAN from the list. |
| TTL Value | Specifies the time-to-live value.<br><br>**NOTE:** This option is applicable for a Routing filter. | Enter a value. |
| Packet Length | Specifies the length of the packet.<br><br>**NOTE:** This option is applicable for a Routing filter. | Enter a value. |
| **Action** | | |

**Table 3: Term-Advanced Options** *(continued)*

| Table | Function | Your Action |
|---|---|---|
| Counter Name | Specifies the count of the number of packets that pass this filter, term, or policer. | Enter a value. |
| Forwarding Class | Classifies the packet into one of the following forwarding classes:<br>■ assured-forwarding<br>■ best-effort<br>■ expedited-forwarding<br>■ network-control<br>■ user-defined | Select the option from the list. |
| Loss Priority | Specifies the Packet Loss Priority.<br>**NOTE:** Forwarding Class and Loss Priority should be specified together for the same term. | Enter the value. |
| Analyzer | Specifies whether to perform port-mirroring on packets. Port-mirroring copies all packets seen on one switch port to a network monitoring connection on another switch port. | Select the analyzer from the list. |

**Related Topics**

- Configuring Firewall Filters (CLI Procedure)
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX-series Switches
- Verifying That Firewall Filters Are Operational
- Firewall Filters for EX-series Switches Overview