Configuring Firewall Filters (J-Web 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.

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

1. Select Configure > Security > Filters.

   The Firewall Filter Configuration page displays a list of all configured port/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. 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 and Table 3.
Association tab		
Port Associations	Specifies the ports with which the filter is associated. **NOTE:** For a port/VLAN filter type, only Ingress direction is supported for port association.	1. Click Add. 2. Select the direction: Ingress or Egress. 3. Select the ports. 4. Click OK.

Table 1: Create a New Filter *(continued)*

Field	Function	Your Action
VLAN Associations	Specifies the VLANs with which the filter is associated. **NOTE:** Because router firewall filters can be associated with ports only, this section is not displayed for a router firewall filter.	1. Click Add. 2. Select the direction: Ingress or Egress. 3. Select the VLANs. 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. 2. Select the protocols. 3. Click OK.
Source	Specifies the source IP address, MAC address, and available ports. **NOTE:** MAC address is specified only for port/VLAN filters.	To specify the IP address, click Add > IP and enter the IP address. To specify the MAC address, click Add > MAC and enter the MAC address. To specify the ports (interfaces), click Add > Ports and enter the port number. To delete the IP address, MAC address, or port details, select it and click Remove.
Destination	Specifies the destination IP address, MAC address, and available ports. **NOTE:** MAC address is specified only for port/VLAN filters.	To specify the IP address, click Add > IP and enter the IP address. To specify the MAC address, click Add > MAC and enter the MAC address. To specify the ports (interfaces), click Add > Ports and enter the port number. To delete the IP address, MAC address, or port details, select it and click Remove.
Action	Specifies the packet action for the term.	Select one: ■ Accept ■ Discard
More	Specifies advanced configuration options for the filter.	Select the match conditions as specified in Table 3. Select the packet action for the term as specified in Table 3.

Table 3: Advanced Options for Terms

Table	Function	Your Action
ICMP Type	Specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition 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 a value from the list.
DSCP	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.
Precedence	Specifies IP precedence. **NOTE:** IP precedence and DSCP number cannot be specified together for the same term.	Select the option from the list.
IP Options	Specifies the presence of the options field in the IP header.	Select the option from the list.
Interface	Specifies the interface on which the packet is received.	Select the interface from the list.
Ether type	Specifies the Ethernet type field of a packet. **NOTE:** This option is not applicable for a routing filter.	Select a value from the list.
Dot 1q user priority	Specifies the user-priority field of the tagged Ethernet packet. User-priority values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed) ■ background (1)—Background ■ best-effort (0)—Best effort ■ controlled-load (4)—Controlled load ■ excellent-load (3)—Excellent load ■ network-control (7)—Network control reserved traffic ■ standard (2)—Standard or Spare ■ video (5)—Video ■ voice (6)—Voice **NOTE:** This option is not applicable for a routing filter.	Select a value from the list.
VLAN	Specifies the VLAN to be associated with the packet. **NOTE:** This option is not applicable for a routing filter.	Select the VLAN from the list.
TCP Flags	Specifies one or more TCP flags. **NOTE:** TCP flags are supported on ingress ports, VLANs, and router interfaces.	Select the option TCP Initial or enter a combination of TCP flags.

Table 3: Advanced Options for Terms *(continued)*

Table	Function	Your Action
Fragmentation Flags	Specifies the IP fragmentation flags. **NOTE:** Fragmentation flags are supported on ingress ports, VLANs, and router interfaces.	Select either the option is-fragment or enter a combination of fragment action flags.
Dot1q tag	Specifies the value for tag field in the Ethernet header. Values can be from 1 through 4095. **NOTE:** This option is not applicable for a routing filter.	Enter the value.
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: ■ assured-forwarding ■ best-effort ■ expedited-forwarding ■ network-control ■ user-defined	Select the option from the list.
Loss priority	Specifies the packet loss priority. **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 entering one switch port to a network monitoring connection on another switch port.	Select the analyzer (port mirroring configuration) 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
- Firewall Filter Match Conditions and Actions for EX Series Switches

Published: 2009-07-28