Firewall Filters for EX Series Switches Overview

Firewall filters provide rules that define whether to permit, deny, or forward packets that are transiting an interface on a Juniper Networks EX Series Ethernet Switch from a source address to a destination address. You configure firewall filters to determine whether to permit, deny, or forward traffic before it enters or exits a port, VLAN, or Layer 3 (routed) interface to which the firewall filter is applied. An *ingress* firewall filter is a filter that is applied to packets that are entering a network. An *egress* firewall filter is a filter that is applied to packets that are exiting a network. You can configure firewall filters to subject packets to filtering, class-of-service (CoS) marking (grouping similar types of traffic together, and treating each type of traffic as a class with its own level of service priority), and traffic policing (controlling the maximum rate of traffic sent or received on an interface).

Firewall Filter Types

The following firewall filter types are supported for EX Series Switches:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 switch ports. You can apply port firewall filters in both ingress and egress directions on a physical port.
- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, and leave a VLAN. You can apply VLAN firewall filters in both ingress and egress directions on a VLAN. VLAN firewall filters are applied to all packets that are forwarded to or forwarded from the VLAN.
- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on Layer 3 (routed) interfaces and routed VLAN interfaces (RVI). You can also apply a router firewall filter in ingress direction on the loopback interface.

NOTE: Firewall filters configured on loopback interfaces are applied to packets transiting network interfaces only; they are not applied to packets transiting the management interface (me0).

To apply a firewall filter, you must:

1. Configure the firewall filter.
2. Apply the firewall filter to a port, VLAN, or Layer 3 interface.

Firewall Filter Components

In a firewall filter, you first define the family address type, (ethernet-switching or inet), and then you define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Each term consists of the following components:

- Match conditions—Specifies the values or fields that the packet must contain. You can define various match conditions, including the IP source address field, IP destination address field, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field, IP protocol field, Internet Control Message Protocol (ICMP) packet type, TCP flags, and interfaces.
- Action—Specifies what to do if a packet matches the match conditions. Possible actions are to accept or discard the packet or to send the packet to a specific virtual routing interface. In addition, packets can be counted to collect statistical information. If no action is specified for a term, the default action is to accept the packet.

NOTE: For Juniper Networks EX3200 and EX4200 Ethernet Switches, the maximum number of terms allowed per firewall filter is 2048. For Juniper Networks EX8200 Ethernet Switches, the maximum number of terms allowed per firewall filter is 32768. If you attempt to configure a firewall filter that exceeds these limits, the switch returns an error message when you commit the configuration.

Firewall Filter Processing

The order of the terms within a firewall filter is important. Packets are tested against each term in the order in which the terms are listed in the firewall filter configuration. When a firewall filter contains multiple terms, the switch takes a top-down approach and compares a packet against the first term in the firewall filter. If the packet matches the first term, the switch executes the action defined by that term to either permit or deny the packet, and no other terms are evaluated. If the switch does not find a match between the packet and first term, it then compares the packet to the next term in the firewall filter by using the same match process. If no match occurs between the packet and the second term, the switch continues to compare the packet to each successive term defined in the firewall filter until a match is found. If a packet does not match any terms in a firewall filter, the default action is to discard the packet.

Related Topics

- Understanding Planning of Firewall Filters
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches
- Understanding How Firewall Filters Are Evaluated
- Understanding Firewall Filter Match Conditions
- Understanding the Use of Policers in Firewall Filters
- Understanding Filter-Based Forwarding for EX Series Switches

- 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

---

Published: 2009-07-28