

Chapter 8

Firewall Filter Overview

Firewall filters allow you to filter packets based on their components and to perform an action on packets that match the filter.



Note

The JUNOS Internet software provides a *policy framework*, which is a collection of JUNOS policies that include routing policies and firewall filter policies. These policies share some fundamental similarities. (For information about the similarities and differences among these policies, see “Policy Framework Overview” on page 3.) However, when referring to a firewall filter policy in the firewall filters part of the manual, the term *firewall filter* is used.

Depending on the hardware configuration of the router, you can use firewall filters for the following purposes:

On routers equipped with an Internet Processor II ASIC, you can control *data packets*, which are chunks of data transiting the router as they are forwarded from a source to a destination.

On all routers, you can control the *local packets*, which are chunks of data that are destined for or sent by the Routing Engine.

With the Internet Processor II ASIC, you can use filters on data packets passing through the router to provide protocol-based firewalls, thwart denial-of-service (DoS) attacks, prevent falsifying of source addresses, create access control lists, and implement rate limiting (policing). (Use the `show chassis hardware` command to determine whether a router has an Internet Processor or an Internet Processor II ASIC.)

You can use the filters to restrict the local packets that pass from the router’s physical interfaces to the Routing Engine. Such filters are useful in protecting the IP services that run on the Routing Engine, such as telnet, secure shell (ssh), and the Border Gateway Protocol (BGP), from denial-of-service attacks. You can define input filters, which affect only inbound traffic destined for the Routing Engine, and output filters, which affect only outbound traffic sent from the Routing Engine. You can also use policing, or rate limiting, to provide a finer level of control over local packets destined for the Routing Engine.



Note

In the remainder of the firewall filters part of this manual, the term *packets* refers to both data and local packets unless explicitly stated otherwise.

You can apply firewall filters to packets entering or leaving the router on one, more than one, or all interfaces. For each interface, you can apply a firewall filter to incoming or outgoing traffic, or both, and the same filter can be used for both.

You can define firewall filters that apply to Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6), or Multiprotocol Label Switching (MPLS) traffic.

There is no limit to the number of filters and counters you can set, but there are some practical considerations. More counters require more terms, and a large number of terms can take a long time to process during a commit. However, filters with more than 1000 terms and counters have been implemented successfully.

Firewall Filter Components

In a firewall filter, you first define the address structure type (IPv4, IPv6, or MPLS), 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 two components:

Match conditions—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, IP options, TCP flags, incoming logical or physical interface, and outgoing logical or physical interface.

Action—Specifies what to do if a packet matches the match conditions. Possible actions are to accept, discard, or reject a packet, go to the next term, or take no action. In addition, statistical information can be recorded for a packet: it can be counted, logged, or sampled.

The order of the terms within a firewall filter is significant. Packets are tested against each term in the order in which they are listed in the configuration. When the first matching conditions are found, the action associated with that term is applied to the packet and the evaluation of the firewall filter ends, unless the next term action modifier is included. If the next term action is included, the matching packet is then evaluated against the next term in the firewall filter; otherwise, the matching packet is not evaluated against subsequent terms in the firewall filter.

If, after all terms are evaluated, a packet matches no terms in a filter, the packet is silently discarded.

If a packet arrives on an interface and a firewall filter is not configured for the incoming traffic on that interface, the packet is accepted by default.

Although policing, traffic sampling, and forwarding are configured as firewall filters, they are documented in separate parts of this manual. For information about policing, see “Policer Configuration” on page 187. For information about traffic sampling and forwarding, see “Traffic Sampling and Forwarding Configuration” on page 215.