

Chapter 22

Firewall Filter Overview

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

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

- On all routers, you can control the packets destined to or sent by the Routing Engine.

- On routers equipped with an Internet Processor II ASIC only, you can control packets passing through the router.

You can use the filters to restrict the 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, ssh, and 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.

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

You can apply firewall filters to input traffic or to traffic leaving the router on one, more than one, or all interfaces. You can apply the same filter to multiple interfaces.

Firewall Filter Components

In a firewall filter, 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, the IP destination address field, the TCP or UDP source port field, the IP protocol field, the 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, or to take no action. In addition, statistical information can be recorded for a packet: it can be counted, logged, or sampled.

• The ordering of the terms within a firewall filter is significant. Packets are tested against each term in the order they are listed in the configuration. When the first matching conditions are found, the action associated with that term is applied to the packet.

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

• Policing, or rate-limiting, is a special application of a firewall filter. In this case the match conditions are the rate-limiting statements that you define, and the actions to discard or mark a packet for subsequent processing take effect if the defined limits are exceeded by the traffic.