

Chapter 22

IPv6 Firewall Filtering

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



Note

The JUNOS Internet software provides a *policy frame work*, which is a collection of JUNOS policies that include routing policies and firewall filter policies. These policies share some fundamental similarities. 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.

This chapter discusses the following topics that provide information for configuring IPv6 filters:

Firewall Filter Overview on page 270

Firewall Filter Configuration Guidelines on page 271

Summary of Firewall Filter Configuration Statements on page 274

For a complete discussion of firewalls, see the *JUNOS Software Configuration Guide: Policy Framework*.

Firewall Filter Overview

With the Internet Processor II ASIC, you can use filters on data packets passing through the router to provide protocol-based firewalls, hinder denial of service (DoS) attacks, prevent falsifying of source addresses, create access control lists, and 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 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, ssh, and 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.

You can apply firewall filters to packets entering or leaving the router on one, more than one, or all interfaces. You can apply the same filter to multiple interfaces. You can apply only one input and one output firewall filter to each interface.

There is no hard 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. Filters with over 1000 terms and counters have been implemented successfully.

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 IPv6 packet must contain. You can define match conditions based on the following components:

IPv6 source address field

IPv6 destination address field

Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field

TCP or UDP destination port field

IP protocol field

Next header field

Traffic class field

Internet Control Message Protocol (ICMP) packet type

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 and the evaluation of the firewall filter ends. 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 interface, by default, the packet is accepted.

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.

For a complete discussion of routing policy, see the *JUNOS Software Configuration Guide: Policy Framework*.

Firewall Filter Configuration Guidelines

You configure IPv6 firewall filters the same way you configure IPv4 firewall filters. An IPv6 filter can filter on IPv6-specific fields as well as IPv4 fields. In the firewall family statement, you can specify `inet6` for IPv6 filters.

The following Requests for Comments (RFCs) define the standards supported by certain aspects of the filtering software:

RFC 792, *Internet Control Message Protocol (ICMP)*

RFC 2474, *Definition of the Differentiated Services (DS) Field*

RFC 2475, *An Architecture for Differentiated Services*

RFC 2597, *Assured Forwarding PHB*

RFC 2598, *An Expedited Forwarding PHB*

RFC 2460, *Internet Protocol Version 6*

For a complete description of configuring firewalls, see the *JUNOS Software Configuration Guide: Policy Framework*.

Minimum Firewall Filter Configuration

To configure an IPv6 firewall filter, you must perform at least the following tasks:

Configure an IPv6 firewall filters—To configure firewall filters, include one or more filter statements at the [edit firewall family inet6] hierarchy level:

```
[edit firewall family inet6]
filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}
```

Apply IPv6 firewall filters to interfaces—Firewall filters control local packets to and from the Routing Engine if they are applied to the loopback interface, lo0. With the Internet Processor II ASIC, firewall filters can control data packets through the router when they are applied to an external interface. To have an IPv6 firewall filter take effect, you must apply it to an interface by including the filter statement at the [edit interfaces interface-name unit logical-unit-number family inet6] hierarchy level:

```
interfaces {
  interface-name {
    unit logical-unit-number {
      family inet6 {
        filter {
          input filter-name;
          output filter-name;
        }
      }
    }
  }
}
```

Filter Match Statement

In a firewall filter term, the from statement defines conditions used to match the components of an IPv6 packet:

```
[edit firewall family inet6 filter filter-name]
term term-name {
  from {
    match-conditions;
  }
}
```

You can specify zero or more match conditions in a single from statement. For a match to occur, the packet must match all the conditions in the term.

The from statement is optional. If you omit it, all packets are considered to match.

Filter Match Conditions

In the from statement in the firewall filter term, you specify conditions that the packet must match for the action in the then statement to be taken. All conditions in the from statement must match for the action to be taken. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify no match conditions in a term, that term matches all packets.

An individual condition in a from statement can contain a list of values. For example, you can specify numeric ranges or multiple source or destination addresses. When a condition defines a list of values, a match occurs if one of the values in the list matches the packet.

Individual conditions in a from statement can be negated. When you negate a condition, you are defining an explicit mismatch. If a packet matches a negated condition, it is immediately considered not to match the from statement, and the next term in the filter is evaluated, if there is one; if there are no more terms, the packet is discarded.

You can filter on the following IPv6-specific match conditions:

Next header field

Traffic class

You can also filter on the following existing IPv4 match conditions:

Source and destination address

ICMP type

Source and destination port

Interface group

Packet length



Note

JUNOS software does not filter on IPv6 extension headers.

Summary of Firewall Filter Configuration Statements

The following descriptions explain each of the firewall filter configuration statements. The statements are organized alphabetically.

filter

Syntax filter *filter-name* {
 term *term-name* {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
 }

Hierarchy Level [edit firewall]

Description Configure firewall filters.

Options *filter-name*—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

The remaining statements are explained separately.

Usage Guidelines See “Firewall Filter Configuration Guidelines” on page 271.

Required Privilege Level firewall—To view this statement in the configuration.
 firewall-control—To add this statement to the configuration.

firewall

Syntax firewall family inet6 { ... }

Hierarchy Level [edit]

Description Configure IPv6 firewall filters.

The remaining statements are explained separately.

Usage Guidelines See “Firewall Filter Configuration Guidelines” on page 271.

Required Privilege Level firewall—To view this statement in the configuration.
 firewall-control—To add this statement to the configuration.

term

Syntax	<pre>term <i>term-name</i> { from { <i>match-conditions</i>; } then { <i>actions</i>; <i>action-modifiers</i>; } }</pre>
Hierarchy Level	[edit firewall family inet6 filter <i>filter-name</i>]
Description	Define a firewall filter term.
Options	<p><i>actions</i>—(Optional) An action to take if conditions match. If you do not specify an action, the packets that match the conditions in the from statement are accepted.</p> <p><i>action-modifiers</i>—(Optional) One or more actions to perform on a packet.</p> <p><i>from</i>—(Optional) Match packet fields to values. If not included, all packets are considered to match and the actions and action modifiers in the then statement are taken.</p> <p><i>match-conditions</i>—One or more conditions to use to make a match.</p> <p><i>term-name</i>—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><i>then</i>—(Optional) Actions to take on matching packets. If not included and a packet matches all the conditions in the from statement, the packet is accepted.</p>
Usage Guidelines	See "Firewall Filter Configuration Guidelines" on page 271.
Required Privilege Level	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>

