

## Chapter 1

# Policy Framework Overview

The JUNOS software provides a *policy framework*, which is a collection of JUNOS policies that allows you to control flows of routing information and packets. The policy framework is composed of the following policies:

Routing policy—Allows you to control the routing information between the routing protocols and the routing tables and between the routing tables and the forwarding table

Firewall filter policy—Allows you to control packets transiting the router to a network destination and packets destined for and sent by the router



**NOTE:** The term *firewall filter policy* is used here to emphasize that a firewall filter is a policy and shares some fundamental similarities with a routing policy. However, when referring to a firewall filter policy in the rest of this manual, the term *firewall filter* is used.

---

This chapter discusses the following topics related to understanding the JUNOS policy framework:

Router Flows Affected by Policies on page 4

Policy Architecture on page 6

Comparison of Routing Policies and Firewall Filters on page 9

## Router Flows Affected by Policies

---

The JUNOS policies affect the following router flows:

Flow of routing information between the routing protocols and the routing tables and between the routing tables and the forwarding table. The Routing Engine handles this flow. *Routing information* is the information about routes learned by the routing protocols from a router's neighbors. This information is stored in routing tables and is subsequently advertised by the routing protocols to the router's neighbors. Routing policies allow you to control the flow of this information.

Flow of data packets in and out of the router's physical interfaces. The Packet Forwarding Engine handles this flow. *Data packets* are chunks of data that transit the router as they are being forwarded from a source to a destination. When a router receives a data packet on an interface, it determines where to forward the packet by looking in the forwarding table for the best route to a destination. The router then forwards the data packet toward its destination through the appropriate interface. Firewall filters allow you to control the flow of these data packets.

Flow of local packets from the router's physical interfaces and to the Routing Engine. The Routing Engine handles this flow. *Local packets* are chunks of data that are destined for or sent by the router. Local packets usually contain routing protocol data, data for IP services such as telnet or secure shell (ssh), and data for administrative protocols such as the Internet Control Message Protocol (ICMP). When the Routing Engine receives a local packet, it forwards the packet to the appropriate daemon or to the kernel, which are both part of the Routing Engine, or to the Packet Forwarding Engine. Firewall filters allow you to control the flow of these local packets.

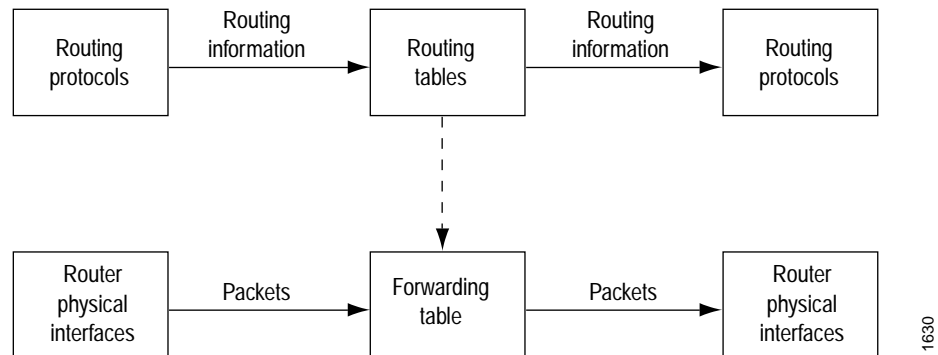


**NOTE:** In the rest of this chapter, the term *packets* refers to both data and local packets unless explicitly stated otherwise.

---

Figure 1 illustrates the flows through the router. Although the flows are very different from each other, they are also interdependent. Routing policies determine which routes are placed in the forwarding table. The forwarding table, in turn, has an integral role in determining the appropriate physical interface through which to forward a packet.

Figure 1: Flows of Routing Information and Packets



You can configure routing policies to control which routes the routing protocols place in the routing tables and to control which routes the routing protocols advertise from the routing tables (see Figure 2). The routing protocols advertise active routes only from the routing tables. (An *active route* is a route that is chosen from all routes in the routing table to reach a destination. For information about the active route selection process, see the *JUNOS Routing Protocols Configuration Guide*.)

You can also use routing policies to do the following:

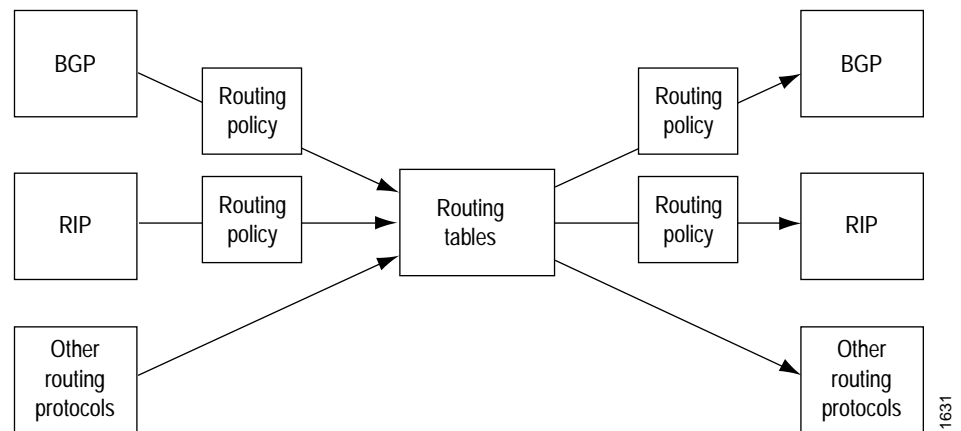
- Change specific route characteristics, which allow you to control which route is selected as the active route to reach a destination. In general, the active route is also advertised to a router's neighbors.

- Change to the default Border Gateway Protocol (BGP) route flap-damping values.

- Perform per-packet load balancing.

- Enable class of service (CoS).

Figure 2: Routing Policies to Control Routing Information Flow



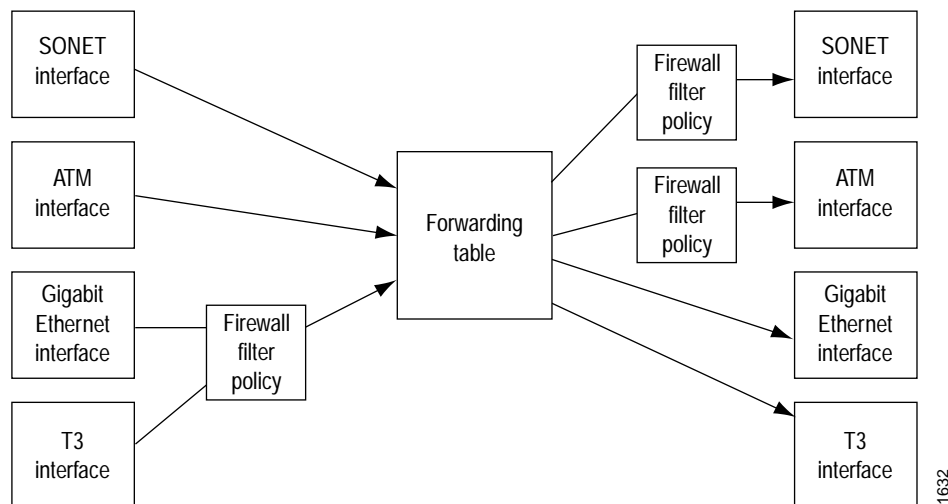
You can configure firewall filters to control the following (see Figure 3):

Which data packets are accepted on and transmitted from the physical interfaces. To control the flow of data packets, you apply firewall filters to the physical interfaces.

Which local packets are transmitted from the physical interfaces and to the Routing Engine. To control local packets, you apply firewall filters on the loopback interface, which is the interface to the Routing Engine.

Firewall filters provide a means of protecting your router from excessive traffic transiting the router to a network destination or destined for the Routing Engine. Firewall filters that control local packets can also protect your router from external aggressions such as denial-of-service attacks.

**Figure 3: Firewall Filters to Control Packet Flow**



## Policy Architecture

A *policy* is a mechanism in the JUNOS policy framework that allows you to configure criteria against which something can be compared and an action that is performed if the criteria are met.

All policies in the JUNOS policy framework share the following architecture and configuration fundamentals:

Control Points on page 7

Policy Components on page 8

Default Policies and Actions on page 8

Configuration Tasks on page 9

Policy Configuration Recommendations on page 9



**NOTE:** This section highlights the fundamental architecture that all policies share. Note, however, that the implementation details of routing policies and firewall filters are very different. For information about these differences, see “Comparison of Routing Policies and Firewall Filters” on page 9.

## Control Points

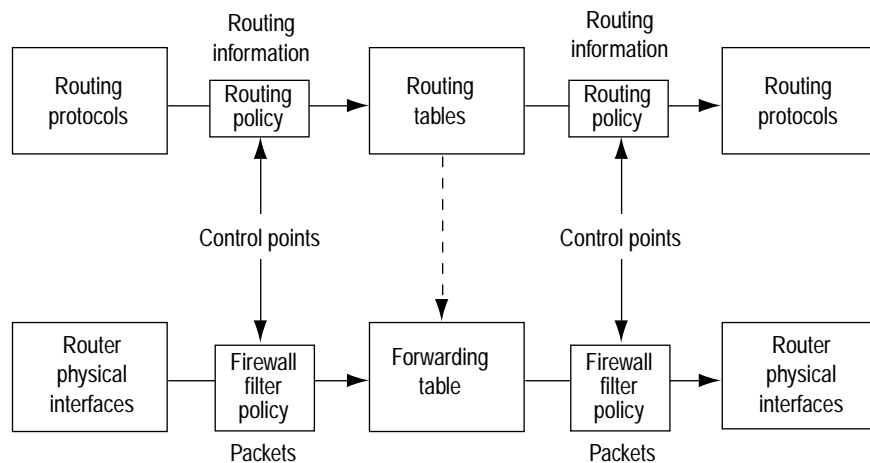
All policies provide two points at which you can control routing information or packets through the router (see Figure 4). These control points allow you to control the following:

Routing information before and after it is placed in the routing table.

Data packets before and after a forwarding table lookup.

Local packets before and after they are received by the Routing Engine. (Figure 4 appears to depict only one control point but because of the bidirectional flow of the local packets, two control points actually exist.)

**Figure 4: Policy Control Points**



1633

Because there are two control points, you can configure policies that control the routing information or data packets before and after their interaction with their respective tables, and policies that control local packets before and after their interaction with the Routing Engine. *Import routing policies* control the routing information that is placed in the routing tables, while *export routing policies* control the routing information that is advertised from the routing tables. *Input firewall filters* control packets that are received on a router interface, while *output firewall filters* control packets that are transmitted from a router interface.

## Policy Components

All policies are composed of the following components that you configure:

*Match conditions*—Criteria against which a route or packets are compared. You can configure one or more criteria. If all criteria match, one or more actions are applied.

*Actions*—What happens if all criteria match. You can configure one or more actions.

*Terms*—Named structures in which match conditions and actions are defined. You can define one or more terms.

For more information about these concepts and how they fit into the context of their respective policies, see “Configuring a Routing Policy” on page 24 and “Firewall Filter Components” on page 154.

The policy framework software evaluates each incoming and outgoing route or packet against the match conditions in a term. If the criteria in the match conditions are met, the defined action is taken.

In general, the policy framework software compares the route or packet against the match conditions in the first term in the policy, then goes on to the next term, and so on. (For specific information about when the evaluation process ends for each policy, see “Comparison of Routing Policies and Firewall Filters” on page 9.) Therefore, the order in which you arrange terms in a policy is relevant.

The order of match conditions within a term is not relevant because a route or packet must match all match conditions in a term for an action to be taken.

## Default Policies and Actions

If an incoming or outgoing route or packet arrives and there is no explicitly configured policy related to the route or to the interface upon which the packet arrives, the action specified by the default policy is taken. A *default policy* is a rule or a set of rules that determine if the route is placed in or advertised from the routing table, or if the packet is accepted into or transmitted from the router interface.

All policies also have default actions in case one of the following situations arises during policy evaluation:

A policy does not specify a match condition.

A match occurs, but a policy does not specify an action.

A match does not occur with a term in a policy and subsequent terms in the same policy exist.

A match does not occur by the end of a policy.

## Configuration Tasks

All policies share a two-step configuration process:

**Define the policy**—Define the policy components. The components include criteria against which routes or packets are compared and actions that are performed if the criteria are met. For more information, see “Policy Components” on page 8.

**Apply the policy**—Apply the policy to whatever moves the routing information or packets through the router, for example, the routing protocol or the router interface.



**NOTE:** A defined policy does not take effect until you apply it.

---

## Policy Configuration Recommendations

The JUNOS policy architecture is simple and straightforward. However, the actual implementation of each policy adds layers of complexity to the policy as well as adding power and flexibility to your router’s capabilities. Configuring a policy has a major impact on the flow of routing information or packets within and through the router. For example, you can configure a routing policy that does not allow routes associated with a particular customer to be placed in the routing table. As a result of this routing policy, the customer routes are not used to forward data packets to various destinations and the routes are not advertised by the routing protocol to neighbors.

Before configuring a policy, determine what you want to accomplish with it and thoroughly understand how to achieve your goal using the various match conditions and actions. Also, make certain that you understand the default policies and actions for the policy you are configuring.

## Comparison of Routing Policies and Firewall Filters

---

Although routing policies and firewall filters share an architecture, as described in “Policy Architecture” on page 6, their purposes, implementation, and configuration are different. Table 2 on page 10 describes their purposes. Table 3 on page 10 compares the implementation details for routing policies and firewall filters, highlighting the similarities and differences in their configuration.

For complete information about routing policies, see “Routing Policies” on page 15. For complete information about firewall filters, see “Firewall Filters” on page 151.

**Table 2: Purpose of Routing Policies and Firewall Filters**

| Policies         | Source   | Policy Purpose   |
|------------------|--|--|
| Routing policies | Routing information is generated by internal networking peers.   | To control the size and content of the routing tables, which routes are advertised, and which routes are considered the best to reach various destinations.                                      |
| Firewall filters | Packets are generated by internal and external devices through which hostile attacks can be perpetrated. | To protect your router and network from excessive incoming traffic or hostile attacks that can disrupt network service, and to control which packets are forwarded from which router interfaces. |

**Table 3: Implementation Differences Between Routing Policies and Firewall Filters**

| Policy Architecture                                   | Routing Policy Implementation   | Firewall Filter Implementation   |
|---|---|--|
| Control points  | Control routing information that is placed in the routing table with an import routing policy and advertised from the routing table with an export routing policy.  | Control packets that are accepted on a router interface with an input firewall filter and that are forwarded from an interface with an output firewall filter.   |
| Configuration tasks:<br>Define policy<br>Apply policy | <p>Define a policy that contains terms, match conditions, and actions.</p> <p>Apply one or more export or import policies to a routing protocol. You can also apply a <i>policy expression</i>, which uses Boolean logical operators with multiple import or export policies.</p> <p>You can also apply one or more export policies to the forwarding table.</p>                                  | <p>Define a policy that contains terms, match conditions, and actions.</p> <p>Apply one input or output firewall filter to a physical interface or physical interface group to filter data packets received by or forwarded to a physical interface (on routing platforms with an Internet Processor II application-specific integrated circuit [ASIC] only).</p> <p>You can also apply one input or output firewall filter to the routing platform's loopback interface, which is the interface to the Routing Engine (on all routing platforms). This allows you to filter local packets received by or forwarded from the Routing Engine.</p> |
| Terms   | <p>Configure as many terms as desired. Define a name for each term.</p> <p>Terms are evaluated in the order in which you specify them.</p> <p>Evaluation of a policy ends after a packet matches the criteria in a term and the defined or default policy action of accept or reject is taken. The route is not evaluated against subsequent terms in the same policy or subsequent policies.</p> | <p>Configure as many terms as desired. Define a name for each term.</p> <p>Terms are evaluated in the order in which you specify them.</p> <p>Evaluation of a firewall filter ends after a packet matches the criteria in a term and the defined or default action is taken. The packet is not evaluated against subsequent terms in the firewall filter.</p>  |

| Policy Architecture | Routing Policy Implementation  | Firewall Filter Implementation   |
|---------------------|--|--|
| Match conditions    | <p>Specify zero or more criteria that a route must match. You can specify criteria based on source, destination, or properties of a route. You can also specify the following match conditions, which require more configuration:</p> <ul style="list-style-type: none"> <li>Autonomous system (AS) path expression—A combination of AS numbers and regular expression operators.</li> <li>Community—A group of destinations that share a common property.</li> <li>Prefix list—A named list of prefixes.</li> <li>Route list—A list of destination prefixes.</li> <li>Subroutine—A routing policy that is called repeatedly from other routing policies.</li> </ul> | <p>Specify zero or more criteria that a packet must match. You must match various fields in the packet's header. The fields are grouped into the following categories:</p> <ul style="list-style-type: none"> <li>Numeric values, such as port and protocol numbers.</li> <li>Prefix values, such as IP source and destination prefixes.</li> <li>Bit-field values—Whether particular bits in the fields are set, such as IP options, Transmission Control Protocol (TCP) flags, and IP fragmentation fields. You can specify the fields using Boolean logical operators.</li> </ul> |

| Policy Architecture | Routing Policy Implementation   | Firewall Filter Implementation  |
|---------------------|---|---|
| <p>Actions</p>      | <p>Specify zero or one action to take if a route matches all criteria. You can specify the following actions:</p> <p>Accept—Accept the route into the routing table, and propagate it. After this action is taken, the evaluation of subsequent terms and policies ends.</p> <p>Reject—Do not accept the route into the routing table, and do not propagate it. After this action is taken, the evaluation of subsequent terms and policies ends.</p> <p>In addition to the actions described above, you can also specify zero or more of the following types of actions:</p> <p>Next term—Evaluate the next term in the routing policy.</p> <p>Next policy—Evaluate the next routing policy.</p> <p>Actions that manipulate characteristics associated with a route as the routing protocol places it in the routing table or advertises it from the routing table.</p> <p>Trace action, which logs route matches.</p> | <p>Specify zero or one action to take if a packet matches all criteria. (We recommend that you always explicitly configure an action.) You can specify the following actions:</p> <p>Accept—Accept a packet.</p> <p>Discard—Discard a packet silently, without sending an ICMP message.</p> <p>Reject—Discard a packet, and send an ICMP destination unreachable message.</p> <p>Routing instance—Specify a routing table to which packets are forwarded.</p> <p>Next term—Evaluate the next term in the firewall filter.</p> <p>In addition to zero or one of the actions described above, you can also specify zero or more action modifiers. You can specify the following action modifiers:</p> <p>Count—Add packet to a count total.</p> <p>Forwarding class—Set the packet forwarding class to a specified value from 0 through 3.</p> <p>IPSec security association—Used with the source and destination address match conditions, specify an IP Security (IPSec) security association (SA) for the packet.</p> <p>Log—Store the header information of a packet on the Routing Engine.</p> <p>Loss priority—Set the packet loss priority (PLP) bit to a specified value, 0 or 1.</p> <p>Policer—Apply rate-limiting procedures to the traffic.</p> <p>Sample—Sample the packet traffic.</p> <p>Syslog—Log an alert for the packet.</p> |

| Policy Architecture          | Routing Policy Implementation   | Firewall Filter Implementation   |
|------------------------------|---|--|
| Default policies and actions | <p>If an incoming or outgoing route arrives and a policy related to the route is not explicitly configured, the action specified by the default policy for the associated routing protocol is taken.</p> <p>The following default actions exist for routing policies:</p> <ul style="list-style-type: none"> <li>If a policy does not specify a match condition, all routes evaluated against the policy match.</li> <li>If a match occurs but the policy does not specify an accept, reject, next term, or next policy action, one of the following occurs: <ul style="list-style-type: none"> <li>The next term, if present, is evaluated.</li> <li>If no other terms are present, the next policy is evaluated.</li> <li>If no other policies are present, the action specified by the default policy is taken.</li> </ul> </li> <li>If a match does not occur with a term in a policy and subsequent terms in the same policy exist, the next term is evaluated.</li> <li>If a match does not occur with any terms in a policy and subsequent policies exist, the next policy is evaluated.</li> <li>If a match does not occur by the end of a policy and no other policies exist, the accept or reject action specified by the default policy is taken.</li> </ul> | <p>If an incoming or outgoing packet arrives on an interface and a firewall filter is not configured for the interface, the default policy is taken (the packet is accepted).</p> <p>The following default actions exist for firewall filters:</p> <ul style="list-style-type: none"> <li>If a firewall filter does not specify a match condition, all packets are considered to match.</li> <li>If a match occurs but the firewall filter does not specify an action, the packet is accepted.</li> <li>If a match occurs, the defined or default action is taken and the evaluation ends. Subsequent terms in the firewall filter are not evaluated, unless the next term action is specified.</li> <li>If a match does not occur with a term in a firewall filter and subsequent terms in the same filter exist, the next term is evaluated.</li> <li>If a match does not occur by the end of a firewall filter, the packet is discarded.</li> </ul> |

