

Policy Information Model

Policies are made up of conditions and actions that cause the router to handle packets in a certain way.

- Condition—Defines values or fields that a packet must contain before an action is triggered; for example, packet direction, network protocol, source and destination ports, application protocol, source and destination networks, packet length, forwarding class, source and destination class
- Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next interface, apply rate and burst size limits, assign a forwarding class

Here are two examples of policies with conditions and actions:

- A stateful firewall:
 - Condition—Matches input packets to a specific destination network
 - Action—Forwards matching packets
- Controlled access policy that defines the sites that a subscriber can view:
 - Condition—Traffic to and from the restricted site
 - Action—Access to the site is stopped if the site has a restricted rating

The SRC policy information model is designed to consolidate information models from various devices to provide a standard way to configure policies. This way, similar operations on different devices are represented as a single policy action or condition which is translated to device-specific operations. For example, the SRC policy information model provides an action that forwards traffic. This action is translated into actions such as forward, accept, or simple handoff on various routers. For instances in which policy conditions or actions are significantly different, the model provides support for each type of condition or action. For example, because rate-limiting on JUNOS routers is significantly different than policing on JUNOS routing platforms the SRC provides a rate-limit action for JUNOS routers and policer action for JUNOS routing platforms.

For JUNOS routers, SRC policies are translated at the COPS-PR or COPS-XDR level and at the router level. For JUNOS routing platforms, policies are translated at the JUNOS XML on BEEP level and at the router level.

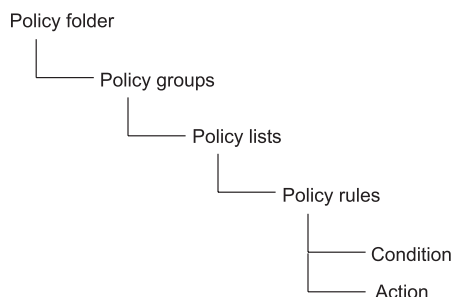
The SRC policy model also lets you simplify policy configuration for policy conditions that classify traffic. For JUNOS and PCMM policies, you can combine different conditions that classify traffic and configure these conditions to use a single action. In addition for JUNOS policies, you can create a condition which actually represents a number of classifiers. The SAE expands the classifier to multiple classifiers before installing them on the router.

For more information about multiple classifiers and expanded classifiers, see Policy Components.

Policy Objects

The SRC policy model is made up of objects that are organized as shown in Figure 1 on page 2.

Figure 1: Policy Object Organization



The following is a description of these objects:

- Policy folders—Used to organize policy groups.
- Policy groups—Hold policy lists. You associate policy groups with a service or with an interface. The SAE sends the information in a policy group to the router, and the router uses the information to create policies that it attaches to router interfaces.
- Policy lists—Used to organize policy rules. You can create policy lists for JUNOS routing platforms, for JUNOSe routers, or for PCMM devices. Whether you create a JUNOS policy list, a JUNOSe policy list, or a PCMM policy list determines the types of policy rules that you can add to the policy list.
- Policy rules—Used to organize the conditions and actions that make up the policy rule. Policy rules consist of conditions that you use to match traffic and actions that specify the action to take if traffic matches the condition. In JUNOS terminology, a policy rule is the same as a *term*.
- Conditions—Define match conditions or classifiers that a packet or packet flow must contain; for example, packet direction, network protocol, application protocol, source and destination networks, packet length, forwarding class, and source and destination class
- Actions—Define the action that the router or CMTS device takes on packets that match conditions

Policy Rules

JUNOSe routers and PCMM devices support one type of policy rule. JUNOS routing platforms support five types of policy rules:

- JUNOS Adaptive Services PIC (ASP)
 - Supports stateful firewall and Network Address Translation (NAT) services.
- JUNOS scheduler

Supports transmission scheduling and rate control parameters on interfaces that support the per-unit scheduler. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular class of traffic.

- JUNOS shaping

Supports setting a shaping rate on PICS that support shaping rate and on interfaces that support the per-unit scheduler.

- JUNOS filter

Supports JUNOS firewall filters.

- JUNOS policer

Supports policing, or rate limiting, by enabling you to limit the amount of traffic that passes into or out of an interface. It is an essential component of firewall filters that is designed to thwart denial-of-service attacks.

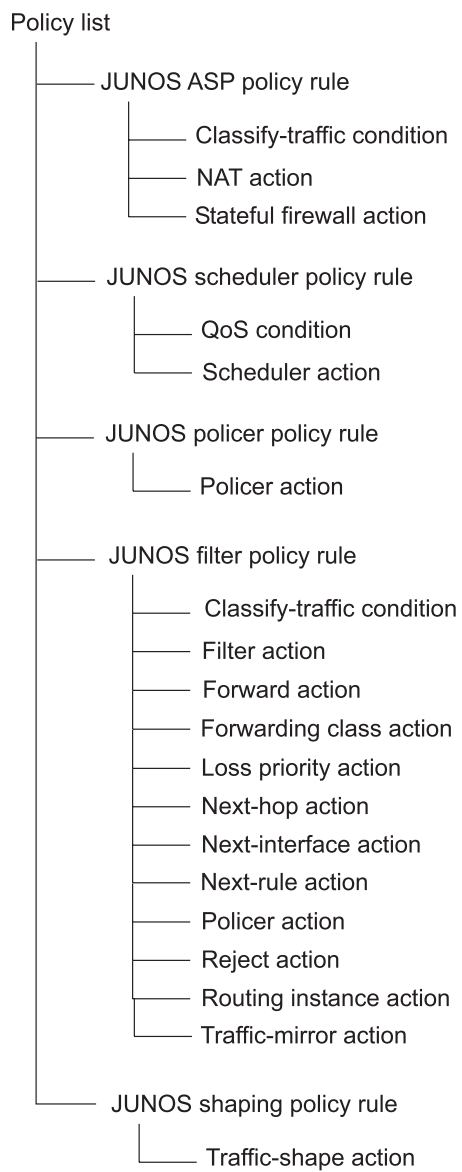
Policing applies two types of rate limits on the traffic:

- Bandwidth—Number of bps permitted, on average.
- Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit.

Supported Conditions and Actions

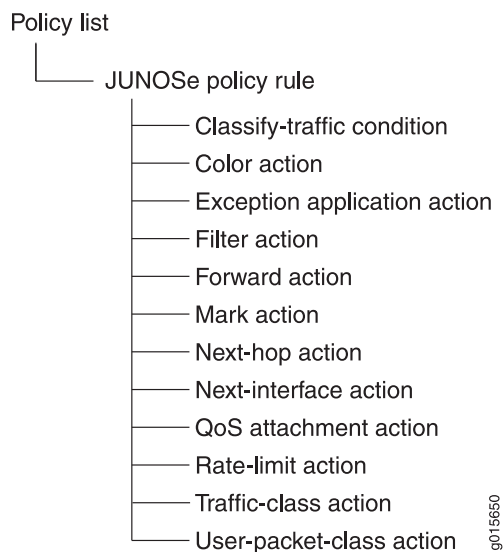
The types of conditions and actions that are available for a policy rule depend on the type of rule. Figure 2 on page 4 shows the types of conditions and actions that are available for JUNOS policy rules. Figure 3 on page 5 shows the types of conditions and actions that are available for JUNOSe policy rules. Figure 4 on page 5 shows the types of conditions and actions that are available for PCMM policy rules.

Figure 2: JUNOS Policy Rules with Supported Conditions and Actions



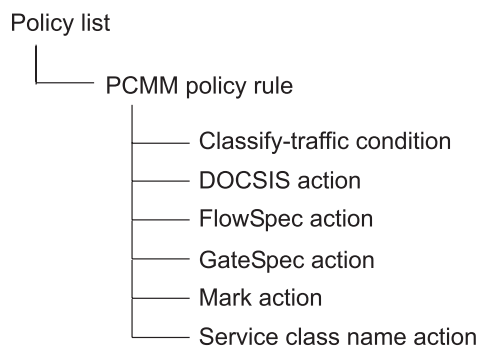
g015745

Figure 3: JUNOS Policy Rules with Supported Conditions and Actions



g015650

Figure 4: PCMM Policy Rules with Supported Conditions and Actions



g015746

Policy Conditions

Policy conditions are values or fields that a packet must contain. If a policy rule does not contain a match condition, all packets are considered to match. There are two types of conditions:

- Classify-traffic condition—Matches can include source and destination addresses or networks; ports, packet types, IP options, TCP flags, network protocol, application protocol
- QoS condition—Matches the forwarding class of the packet

See also [\[Unresolved xref\]](#).

Multiple Classifiers

JUNOS^e and PCMM policy rules can contain multiple classify-traffic conditions. Having multiple classifiers in a policy rule gives you more flexibility for defining services and allows you to use fewer policy rules for some applications.

If multiple policy rules have the same action, but different classify conditions, you can combine the policy rules into one policy rule. You can also set up one policy rule that has multiple classifiers, each for a different subnet or range of addresses.

If you want to collect accounting data on internal versus external traffic, you can configure one policy rule with a set of classifiers for internal traffic and one policy rule with a set of classifiers for external traffic.

Rate-Limiting with Multiple Classifiers

Multiple classifiers give you more flexibility for rate-limiting policies. Without multiple classifiers, you can rate-limit only individual traffic flows. With multiple classifiers, you can rate-limit the aggregate of traffic flows from all sources.

The following example uses multiple classifiers to rate-limit traffic to 1 Mbps for traffic going to two different subnets.

```
Policy List je-in
Policy Rule rate-limiter
ClassifyTrafficCondition CTC1
    SourceNetwork:
        any
    DestinationNetwork:
        ipAddress=172.60.40.0/0.0.0.255
ClassifyTrafficCondition CTC2
    SourceNetwork:
        any
    DestinationNetwork:
        ipAddress=172.60.20.0/0.0.0.255
Rate limit action that limits to 1 Mbps
Policy List je-out
Policy Rule forward
ClassifyTrafficCondition
    DestinationNetwork:
        any
    SourceNetwork:
        any
Forward action
```

Expanded Classifiers

For JUNOS^e policies, you can create classify-traffic conditions that the SAE expands into multiple classifiers before it installs the policy on the router. If you enter a comma-separated list of values in the source and destination network (IP address, mask, and IP operation) or port fields (for port-related protocols), the software creates a classifier for each possible combination of address and port. Note that the software does not expand classifiers for values that are entered as a range.

You would use this feature in policies that are used in IP multimedia subsystem (IMS) environments. You can also use it to simplify the configuration of JUNOSe policies.

For example, the source configuration in the classify-traffic condition in Figure 5 on page 7 would cause the condition to be expanded into four classifiers that have the following combination of source addresses and source ports:

- 192.1.1.0/255.255.255.0 eq 80
- 192.1.1.0/255.255.255.0 eq 8080
- 192.2.1.1/255.255.255.0 eq 80
- 192.2.1.1/255.255.255.0 eq 8080

Figure 5: Classify-Traffic Condition Example for Expanded Classifiers

Source

☐ Grouped IP Address

Network Operation

[1,1]

IP Address

[192.1.1.0, 192.2.1.1]

IP Wildcard

[255.255.255.0, 255.255.255.255]

Port Operation

eq

Port

[80, 8080]

Policy Actions

JUNOS policy rules and PCMM policy rules can have multiple actions. JUNOSe policy rules can have only one action. The types of actions available for a policy rule depend on the type of rule. See “Supported Conditions and Actions” on page 3. The following table is a description of all actions.

Table 1: Policy Actions

Action	Type of Rule	Description
Color	JUNOSe	Specifies the color attribute that is applied to the packet when it passes through the router.
DOCSIS	PCMM	Explicitly specifies the Data over Cable Service Interface Specifications (DOCSIS) parameters of the DOCSIS service flow. It supports all DOCSIS service flow scheduling types.
Exception application	JUNOSe	Specifies an exception to the policy rule for traffic that has a specific application, such as a Web server.
Filter	JUNOS filter	Discards all packets that match the classify-traffic condition.
	JUNOSe	

Table 1: Policy Actions *(continued)*

Action	Type of Rule	Description
FlowSpec	PCMM	Specifies a traffic profile by using a Resource Reservation Protocol (RSVP)-style FlowSpec.
Forward	JUNOS filter JUNOSe	Forwards packets that match the classify-traffic condition; forwards packets to a particular interface and/or a next-hop address.
Forwarding class	JUNOS filter	Assigns a forwarding class to packets that match the classify-traffic condition.
GateSpec	PCMM	Specifies the session class ID in the gate. The session class ID provides a way to group gates into different classes with different authorization characteristics.
Loss priority	JUNOS filter	Assigns a packet loss priority to packets that match the classify-traffic condition.
Mark	PCMM JUNOSe	Sets the ToS field in the IP header for IPv4 packets, or sets the traffic-class field in the header for IPv6 packets to a specified value.
NAT	JUNOS ASP	Specifies the type of network address translation (source dynamic, destination static), IP address ranges, and a port range to restrict port translation when NAT is configured in dynamic-source mode.
Next hop	JUNOS filter JUNOSe	Specifies the IP address of the next hop; used to create a static route on the router; used for captive portal behavior; JUNOS filters support multiple next hops for load balancing.
Next interface	JUNOS filter JUNOSe	Defines an output interface and/or a next-hop address for a policy list; used to create a static route on the router; used for captive portal behavior.
Next rule	JUNOS filter	Causes the router to skip to and evaluate the next rule in the policy list.
Policer	JUNOS policer JUNOS filter	Specifies rate and burst size limits and the action taken if a packet exceeds those limits.
QoS attachment	JUNOSe	Specifies the QoS profile that is applied to the packet when it passes through the router.
Rate limit	JUNOSe	Specifies bandwidth attributes (committed, peak, and excess rates and burst sizes) and the action taken relative to the bandwidth (filter, forward, or mark).
Reject	JUNOS filter	Discards the packet and sends an ICMP destination unreachable message to the client; can set the type of ICMP message to send.
Routing instance	JUNOS filter	Also called filter-based forwarding; directs traffic to a routing instance that is configured on the router.

Table 1: Policy Actions *(continued)*

Action	Type of Rule	Description
Scheduler	JUNOS scheduler	Specifies transmission-scheduling and rate-control parameters. Schedulers define the priority, bandwidth, delay buffer size, rate-control status, and RED drop profiles to be applied to a particular class of traffic.
Service class name	PCMM	Specifies that traffic is controlled by a service class that is configured on the CMTS device.
Stateful firewall	JUNOS ASP	Specifies whether to filter, forward, or reject a packet. If a packet is rejected, a rejection message is returned.
Traffic class	JUNOSe	Specifies the traffic-class profile that is applied to the packet when it passes through the router.
Traffic shape	JUNOS shaping	Specifies the maximum rate of traffic transmitted on an interface.
Traffic mirror	JUNOS filter	Mirrors traffic from a destination to a source or from a source to a destination.
User packet class	JUNOSe	Specifies the user packet class that is applied to the packet when it passes through the router.

Combining Actions

JUNOS policy rules and PCMM policy rules support multiple actions. For example, in PCMM policies, you can combine a mark action with a DOCSIS parameter action, a service schedule action, or a FlowSpec action. In JUNOS policy rules you can combine the forwarding class action, routing instance action, and loss priority action. The result is that packets that match the condition are assigned to a forwarding class, directed to a routing instance on the router, and assigned a packet loss priority.

Only one of the following actions can exist in a policy rule: next-hop action, next-interface action, forward action, filter action, and reject action.

For example, if you add the next-rule action to a policy rule, do not add a next-hop action, next-interface action, forward action, filter action, or reject action to the same policy rule.

Although you can have only one action in a JUNOSe policy rule, you can set up a policy list to take two corresponding actions on a packet. To do so, you create a JUNOSe policy list that has more than one policy rule with the same precedence. For example, you might want a policy rule that marks a packet and a policy rule that forwards the packet to the next interface. Or you could have a policy rule that applies a traffic-class action and a policy rule that forwards the packet to the next hop.

Policy LDAP Schema Model

The policy information model is based on the Policy Core Information Model (PCIM) that is mapped to the Policy Framework LDAP core schema by the IETF. SRC software

extends this model in such a way to be very close to the policy model used by the router. A policy folder might be the base of the policy subtree (*o = policies*, *o = umc*) or an organizationalUnit object, underneath the policy base. Such a policy folder contains group objects consisting of one or many policy lists that contain one or many policy rules. A policy rule consists of policy actions and policy conditions.

The objects policy group, policy list, and policy rule are mapped to structural object classes. Each of those classes is derived from the object class policy. This abstract policy object class is inherited from `d1m1ManagedElement`, which is the top class of the CIM. The policy actions and policy conditions are mapped to auxiliary classes that are attached to the object `policyRule`. The classes `policyActionAuxClass` and `policyConditionAuxClass` are the top classes for any policy action and policy condition. SSP service objects point through the DN pointer to one policy group.

For detailed information about the SRC LDAP schema, see the documentation on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src>.