

Overview of Policy Rules

The type of policy rule that you can create depends on the type and applicability of the policy list in which you create the policy rule. There is only one type of policy rule for PCMM policy lists and AAA policy lists. For JUNOS policy lists, you can create JUNOS IPv4 or JUNOS IPv6 policy rule types. If you are creating a JUNOS secondary input policy, the applicability of policy list must be secondary-input. For JUNOS policy lists, you can create the following policy rule types:

- JUNOS ASP—Applicability of policy list must be both.
- JUNOS FILTER—Applicability of policy list must be input or output.
- JUNOS POLICER—Applicability of policy list must be input or output.
- JUNOS SCHEDULER—Applicability of policy list must be both.
- JUNOS SHAPING—Applicability of policy list must be both.

Before You Configure JUNOS Policy Rules

The following are prerequisites to using policy rules on routers running JUNOS Software:

- JUNOS Scheduler and JUNOS Shaping Policy Rules

Before you use the JUNOS scheduler and JUNOS shaping policy rules, check that your Physical Interface Card (PIC) supports JUNOS scheduling and shaping rate. Also, check that your interface supports the per-unit-scheduler.

You must enable the per-unit-scheduler on the interface. To do so, on routers running JUNOS Software, include the **per-unit-scheduler** statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
per-unit-scheduler;
```

- JUNOS ASP Policy Rules

Before you use the Adaptive Services PIC (ASP) policy rule to create a stateful firewall or NAT policy, you must configure the Adaptive Services PIC on routers running JUNOS Software. For example:

```
sp-0/1/0 {
  unit 0 {
    family inet {
      address 10.10.1.1/32;
    }
  }
}
```

For more information about configuring Adaptive Services PICs, see the *JUNOS Services Interfaces Configuration Guide*.

Setting the Policy Rule Precedence

Policy lists can have more than one policy rule. Policy rules are assigned a precedence that determines the order in which the policy manager applies policy rules. Rules are evaluated from lowest to highest precedence value. Rules with equal precedence are evaluated in random order.

Note that for JUNOS SCHEDULER and JUNOS POLICER policy rules, precedence is not a factor.

The router classifies packets beginning with the classify condition in the policy list that has the policy rule with the lowest precedence.

- If the packet matches the condition, the router applies the policy rule actions to the packet and does not continue to examine further conditions.
- If the packet does not match the condition, the router tries to match the packet with the classify condition in the policy rule with the next higher precedence.
- If the packet does not match any of the classify conditions, it is forwarded. There are some exceptions. For example, in the case of a JUNOS ASP stateful firewall, packets that do not match the classify conditions are dropped. Only matching packets are forwarded.

For routers running JUNOS Software, if you want the router to take two corresponding actions on a packet, you would create a JUNOS policy list that has more than one policy rule with the same precedence. For example, you may 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 and a policy rule that forwards the packet to the next hop.

Related Topics

- Before You Configure SRC Policies
- Policy Information Model
- Adding a Policy Rule (SRC CLI)
- Enabling the Policy Configuration on the SRC CLI
- Example: Creating Access Policies for Subscribers

Published: 2009-09-22