Chapter 21

Configuring and Managing Policies with the C-Web Interface

This chapter describes how to use the C-Web interface to configure and manage policies. You can also use the following to configure and manage policies:

- To use the SRC CLI, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI*.
- To use Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with Policy Editor*.

Topics in this chapter include:

Before You Configure Policies

Building policies is a top-down operation. For example, before you can add a subordinate to the policy group, the policy group itself must exist.

Creating a Worksheet

Before you configure policies, you must determine what information you want to enter and where it will go. It is best to create a worksheet where you can record such things as names, priorities, addresses, and so on.

To create a worksheet:

1. Determine the policy requirements for your system.
2. Consider information that contains (at a minimum) names and parameters for:
   - Policy group
   - Policy list
   - Policy rules
   - Conditions
   - Actions
3. Record the policy information about the worksheet.

Naming Objects

Object names must be unique and must conform to LDAP distinguished name (DN) constraints.

Using the apply-groups Statement

When you use the apply-groups statement on the JUNOS routing platform to apply a configuration group to a hierarchy level in a configuration, you need to make sure that the SAE configuration group (default name is sdx) is in the first position in the apply-groups statement.

Using Expressions

Many of the policy options can take expressions in addition to literal values. If you can enter an expression for an option, the expression type is noted in the documentation for the command. For information about using and formatting expressions, see *Expressions* in *SRC-PE Services and Policies Guide, Chapter 14, Defining and Acquiring Values for Parameters*.

Policy Values

As you are planning your policy configuration, you need to understand how invalid values in policies are handled on JUNOS routing platforms and JUNOSe routers.

SAE to JUNOS Routing Platforms

When the SAE sends policies to JUNOS routing platforms, it uses JUNOScript on the Blocks Extensible Exchange Protocol (BEEP), which is an XML-based protocol. Many of the configuration values in JUNOScript are strings in which the value is a number. If you enter an integer value that is too large, the policy software flags the entry as invalid, but the value is still sent to the router because JUNOScript on BEEP allows for its transmission. The router is the authority that decides whether values are valid for the particular version of the JUNOS software and the routing platform. If the value is too large, the router sends an error message to the SAE.

For example, the valid range for the burst size limit in a policer action is 1,500 to 100,000,000. If you specify a value greater than 100,000,000, it is flagged as invalid. However, as usual, the SRC software attempts to activate the service, but the activation will fail because the burst size is an invalid value on the router.

SAE to JUNOSe Routers

When the SAE sends policies to JUNOSe routers, it uses the Common Open Policy Service (COPS) protocol with specific standard Policy Information Bases (PIBs) and private PIBs. Many of the configuration values in the PIBs are not strings in which the value is a number. Sometimes the numeric range in the PIB is larger than the valid range of values on the router. For integer values in policies, the eventual policy on the router has only the portion of a value that can be converted to an integer in the usable range.

The example below for ToS byte is such a case. From the JUNOSe-IP-PIB:

```
...
JunoseIpPolicyClaclRuleEntry ::= SEQUENCE {
...
junoseIpPolicyClaclRuleTosByte Integer32,
junoseIpPolicyClaclRuleTosMask Integer32,
...
```

If a policy has a literal ToS byte value of 300, the high bits are ignored (or a mask of 255 is used) so that the value used for the ToS byte is 44; that is, 300 minus 256.

Enabling the Policy Configuration on the C-Web Interface

Before you can configure policies with the C-Web interface, you must enable the policy, service, and subscriber editor. To do so:

1. Click **Manage > Enable**.
2. From the Component list, select **editor**.
3. Click **OK**.

Configuring Policy Folders with the C-Web Interface

You use policy folders to organize policy groups.

To create a policy folder:

1. Click **Configure > Policies**.
2. From the Create new list, select **Folder**. Type a name for the new folder, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Groups with the C-Web Interface

Policy groups hold policy lists. You can create policy groups at the Policies level or within policy folders.

To create a policy group:

1. Click **Configure > Policies**. You can add the policy group at the Policies level, or you can expand **Policies** and select a folder for which you want to add the group.
2. From the Create new list, select **Group**. Type a name for the new group, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Lists with the C-Web Interface

When you add a policy list, you specify whether the policy list is for JUNOS routing platforms, JUNOSe routers (junose-ipv4 or junose-ipv6), or a CMTS device (pcmm). The type of policy list that you add controls the type of policy rules that you can add to the policy list.

You create policy lists within policy groups.

To add a policy list:

1. Click **Configure > Policies**.
2. Expand **Policies**, and expand the policy group for which you want to add the list.
3. From the Create new list, select **List**. Type a name for the new list, and click **OK**.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Rules with the C-Web Interface

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. For JUNOSe policy rules, there are two types—IPv6 and IPv6. For PCMM policy rules, there is only one type. 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 JUNOS routing platforms.

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 the JUNOS routing platform, 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 the JUNOS routing platform. 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. For JUNOSe policies, rules with equal precedence are evaluated in the order of creation. For JUNOS policies, 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 JUNOSe routers, if you want the router to take two corresponding actions on a packet, you would create a JUNOSe 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.

Adding a Policy Rule

You create policy rules within policy lists.

To add a policy rule:

1. In the side pane, select a policy list that has already been created and configured.
2. From the Create new list, select **Rule**. Type a name for the new rule, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Classify-Traffic Conditions with the C-Web Interface

You create classify-traffic conditions in JUNOSe policy rules, in JUNOS ASP and JUNOS filter policy rules, and in PCMM policy rules.

The available configuration statements change depending on the type of policy rule that holds the condition and on the type of protocol that you specify.

To configure a classify-traffic condition, do the following:

1. Create a classify-traffic condition. See:
   - Creating a Classify-Traffic Condition on page 211
2. Configure source networks. You can configure source networks in one of two formats. See:
   - Configuring Source Networks on page 212
   - Configuring Source Grouped Networks on page 212
3. Configure destination networks. You can configure destination networks in one of two formats. See:
   - Configuring Destination Networks on page 212
   - Configuring Destination Grouped Networks on page 212

4. Configure protocol conditions. The type of protocol condition that you use depends on your configuration.
   - To configure protocol conditions that do not include ports, see:
     - Configuring Protocol Conditions on page 213
   - To configure protocol conditions that include ports, see:
     - Configuring Protocol Conditions with Ports on page 213
   - To configure protocol conditions in which the protocol that you specify is a parameter, see:
     - Configuring Protocol Conditions with Parameters on page 214
   - To configure protocol conditions in which the protocol is TCP, see:
     - Configuring TCP Conditions on page 214
   - To configure protocol conditions in which the protocol is ICMP, see:
     - Configuring ICMP Conditions on page 215
   - To configure protocol conditions in which the protocol is IGMP, see:
     - Configuring IGMP Conditions on page 215
   - To configure protocol conditions in which the protocol is IPSec, see:
     - Configuring IPSec Conditions on page 215
   - To configure a ToS byte condition, see:
     - Configuring ToS Byte Conditions on page 215
5. For JUNOS filter policies, configure a JUNOS filter condition. See:
   - Configuring JUNOS Filter Conditions on page 216
6. For the stateful firewall and NAT policies, configure an application protocol condition. See:
   - Configuring Application Protocol Conditions on page 216

NOTE: PCMM classifiers support only the following classifiers:

- Source and destination IP addresses
- Network protocol
- Source or destination port
- Type-of-service (ToS) byte and ToS mask

The policy engine ignores all other values.

Before You Configure Classify-Traffic Conditions

If you are configuring classifiers for PCMM policies, you can specify whether the classifier will be used in a PCMM IO2 or IO3 network. By default, the software translates classify-traffic conditions into PCMM IO2 classifiers.

- See *Specifying the PCMM Classifier Type* on page 210.

For JUNOSe policies, you can specify that the SAE expand the classifier into multiple classifiers before it installs the policy on the router.

- See *Enabling Expansion of JUNOSe Classify-Traffic Conditions* on page 210.

Enabling Expansion of JUNOSe Classify-Traffic Conditions

For information about expanded classifiers, see *Expanded Classifiers* in *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

To specify whether or not the SAE expands the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router:

1. Select **Configure**, and expand **Shared > SAE > Configuration > Policy Management Configuration**.
2. Check or clear the Enable JUNOSe Classifier Expansion box, and click **Apply**.

Specifying the PCMM Classifier Type

To specify whether or not the SAE sends to the router classifiers that comply with PCMM I03:

1. Select **Configure**, expand **Shared > SAE > Configuration > Driver**, and select **pcmm**.
2. Check or clear the Disable PCMM I03 Policy box, and click **Apply**.

Specifying Port Access for Traffic Classification

In the SRC software, the way that you specify a range of port numbers greater than or less than a specific value in a traffic classifier is different from the way you define a range in the configuration on JUNOSe routers.

In the C-Web interface, you specify ranges by setting values in the Port Operation boxes.

To specify a range of port numbers greater or less than a specified value, you can:

- Define the full set of port numbers in the range to be allowed.
- Define the full set of port numbers in the range not allowed.

To configure port numbers greater than a defined value by specifying which values are allowed:

1. From the Port Operation list, select **eq**.
2. In the From Port box, enter the range of ports allowed.

   For example, to specify access to all port numbers greater than 10, specify **11..65535**.

To configure port numbers greater than a defined value by specifying which values are not allowed:

1. From the Port Operation list, select **neq**.
2. In the From Port box, enter the range of ports not allowed.

   For example, to specify access to all port numbers greater than 10, specify **1..9**.

To configure port numbers less than a defined value by specifying which values are allowed:

1. From the Port Operation list, select **eq**.
2. In the From Port box, enter the range of ports.

   For example, to specify access to all port numbers less than 10, specify **1..9**.

To configure port numbers less than a defined value by specifying which values are not allowed:

1. From the Port Operation list, select **neq**.
2. In the From Port box, enter the range of ports.

   For example, to specify access to all port numbers less than 10, specify **11..65535**.

Creating a Classify-Traffic Condition

You create classify-traffic conditions within policy rules.

To add a classify-traffic condition:

1. In the side pane, select a policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply.**

Configuring Source Networks

To configure a source network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Source Network**, and select **Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Source Grouped Networks

You can configure source networks in grouped format. For JUNOS ASP policy rules, you must enter source networks in grouped format.

To configure a grouped source network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Source Network**, and select **Group Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Destination Networks

To configure a destination network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Destination Network**, and select **Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Destination Grouped Networks

You can configure destination networks in grouped format. For JUNOS ASP policies rules, you must enter destination networks in grouped format.

To configure a grouped destination network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Destination Network**, and select **Group Network**.

2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions

The procedure in this sections shows how to configure general protocol conditions.

- If your condition includes port numbers, use the procedure in *Configuring Protocol Conditions with Ports* on page 213.

- If your condition consists of a protocol that is assigned with a parameter value, use the procedure in *Configuring Protocol Conditions with Parameters* on page 214.

To configure general protocol conditions in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **Protocol Condition**.

2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions with Ports

To configure general protocol conditions with ports in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **Protocol Port Condition**.

2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports for protocol conditions:

1. In the side pane, expand **Protocol Port Condition > Source Port**, and select **Port**.

2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

3. In the side pane, expand **Protocol Port Condition > Destination Port**, and select **Port**.

4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions with Parameters

Before you assign a parameter for the protocol, you must create a parameter of type protocol and commit the parameter configuration.

To configure a protocol condition that contains a parameter value for the protocol:

1. In the side pane, select a policy rule.
2. From the Create new list, expand a traffic condition, and select **Parameter Protocol Condition**.
3. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
4. (Optional) To configure protocol attributes:
    a. In the side pane, expand **Parameter Protocol Condition**, and select **Proto Attr**.
    b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports:

1. In the side pane, expand **Proto Attr > Source Port**, and select **Port**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
3. In the side pane, expand **Proto Attr > Destination Port**, and select **Port**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring TCP Conditions

To configure TCP conditions:

1. In the side pane, expand a traffic condition, and select **TCP Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports for TCP conditions:

1. In the side pane, expand **TCP Condition > Source Port**, and select **Port**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
3. In the side pane, expand **TCP Condition > Destination Port**, and select **Port**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring ICMP Conditions

To configure ICMP conditions:

1. In the side pane, expand a traffic condition, and select **Icmp Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring IGMP Conditions

To configure IGMP conditions:

1. In the side pane, expand a traffic condition, and select **Igmp Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring IPSec Conditions

You can configure IPSec conditions for JUNOS policy rules.

To configure IPSec conditions:

1. In the side pane, expand a JUNOS traffic condition, and select **Ipsec**.
2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring ToS Byte Conditions

Use this condition to define a particular traffic flow to the service's network for the DA IP field in the IP packet.

The CoS feature on JUNOS routing platforms supports DiffServ as well as six-bit IP header ToS byte settings. The DiffServ protocol uses the ToS byte in the IP header. The most significant six bits of this byte form the Differentiated Services code point (DSCP). The CoS feature uses DSCPs to determine the forwarding class associated with each packet. It also uses the ToS byte and ToS byte mask to determine IP precedence.

To configure ToS byte conditions in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **ToS**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring JUNOS Filter Conditions

To configure traffic match conditions in JUNOS filter policy rules:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. In the side pane, expand the traffic condition, and select **Traffic Match Condition**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Application Protocol Conditions

You can define application protocols for the stateful firewall and NAT services to use in match condition rules. An application protocol defines application parameters by using information from network layer 3 and above. Examples of such applications are FTP and H.323.

Creating and Configuring an Application Protocol Condition

To create and configure an application protocol condition:

1. In the side pane, select an ASP policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. From the Create new list, select Application Protocol Condition. Type a name for the application protocol condition, and click **OK**.
5. Enter information as described in the Help text in the main pane, and click **Apply**.
6. (Optional) To configure protocol attributes:
   a. In the side pane, expand the application protocol condition, and select **Proto Attr**.
   b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
7. (Optional) To configure source ports:
   a. In the side pane, expand **Proto Attr > Destination Port**, and select **Port**.
   b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
8. (Optional) To configure destination ports:

a. In the side pane, expand **Proto Attr > Source Port**, and select **Port**.

b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Using Map Expressions in Application Protocol Conditions

The application protocol condition is a case in which you might use a map expression to define multiple attributes in one option—the application-protocol option. Maps are a list of attributeName = value pairs separated by commas and enclosed in curly brackets. For example, the map {applicationProtocol = "ftp", sourcePort = 123, inactivityTimeout = 60} supplies the application protocol, source port, and inactivity timeout in one option.

Another map {applicationType = "tcp", inactivityTimeout = 60, destinationPort = 80} supplies the protocol, inactivity timeout, and destination port.

You can also create a local parameter, add a map expression as the default value of the parameter, and then enter the local parameter in the application-protocol option.

Configuring QoS Conditions with the C-Web Interface

You can create QoS conditions within JUNOS scheduler policy rules.

To create a QoS condition:

1. In the side pane, select a JUNOS scheduler policy rule.

2. From the Create new list, select **Qos Condition**. Type a name for the QoS condition, and click **OK**.

3. Enter information as described in the Help text in the main pane, and click **Apply.**

Configuring Actions with the C-Web Interface

Actions define the action taken on packets that match conditions in a policy rule. You create actions within policy rules. The type of action that you can create depends on the type of policy rule. See *Supported Conditions and Actions* in *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

Configure the action as described in the following sections:

Configuring DOCSIS Actions

You can configure Data over Cable Service Interface Specifications (DOCSIS) actions for *PacketCable Multimedia Specification* (PCMM) policy rules.

The types of DOCSIS actions that you can create are:

- Best effort
- Downstream
- Non-real-time polling service
- Real-time polling service
- Unsolicited grant service
- Unsolicited grant service with activity detection
- Parameter—This is a DOCSIS action with the service flow scheduling type set to a trafficProfileType parameter. You must enter a trafficProfileType parameter that has been created and committed.

To configure a DOCSIS action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select the type of DOCSIS action that you want to create. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Filter Actions

Use this action to discard packets. You can configure filter actions for JUNOS filters and JUNOSe policy rules.

To configure a filter action:

1. In the side pane, select a JUNOS filter or JUNOSe policy rule.
2. From the Create new list, select **Filter**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring FlowSpec Actions

A FlowSpec is made up of two parts, a traffic specification (TSpec) and a service request specification (RSpec). The TSpec describes the traffic requirements for the flow, and the RSpec specifies resource requirements for the desired service. You can configure FlowSpec actions for PCMM policy rules.

To configure a FlowSpec action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select **Flow Spec**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Forward Actions

Use this action to forward packets, such as packets that are sent by means of a routing table. You can configure forward actions for JUNOS filters and JUNOSe policy rules.

To configure a forward action:

1. In the side pane, select a JUNOS filter or JUNOSe policy rule.
2. From the Create new list, select Forward. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Forwarding Class Actions

You can configure forwarding class actions for JUNOS filter policy rules. The forwarding class action causes the router to assign a forwarding class to packets that match the associated classify-traffic condition.

To configure a forwarding class action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Forwarding Class**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Gate Spec Actions

You can configure GateSpec actions for PCMM policy rules. See *Session Class ID* in *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview* for more information.

To configure a Gate Spec action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select **Gate Spec**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Loss Priority Actions

You can configure loss priority actions for JUNOS filter policy rules. The loss priority action causes the router to assign a packet loss priority to packets that match the associated classify-traffic condition.

To configure a loss priority action:

1. In the side pane, select a JUNOS filter rule.
2. From the Create new list, select **Loss Priority**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Mark Actions

Use this action to mark packets. You can configure mark actions for JUNOSe and PCMM policy rules.

To configure a mark action:

1. In the side pane, select a JUNOSe or PCMM policy rule.
2. From the Create new list, select **Mark**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. Expand the mark action, and select **Info**.
5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring NAT Actions

You can configure NAT actions for JUNOS ASP policy rules. To configure a NAT action:

1. In the side pane, select a JUNOS ASP policy rule.
2. From the Create new list, select **NAT**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. To configure the port range to restrict port translation when the NAT translation type is configured in dynamic-source mode:
   a. In the side pane, select **Port**.
   b. Click create, and enter information as described in the Help text in the main pane, and click **Apply**.
5. To configure the IP address ranges.
   a. In the side pane, select **IP Network**.
   b. In the main pane, click **Create**.
   c. In the side pane, expand **IP Network**, and select **Group Network**.
   d. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Hop Actions

Use this action for the ingress side of the interface to specify the next IP address where the classified packets should go. You can configure next-hop actions for JUNOS filters and JUNOSe policy rules.

Using the Next-Hop Action with the Captive Portal

The captive portal feature is used to intercept HTTP requests from a subscriber to an unauthorized Web resource and redirect the requests to a dedicated Web page, the captive portal page. See *SRC-PE Subscribers and Subscriptions Guide, Chapter 14, Redirecting Subscriber Traffic*.

In a captive portal environment, you would typically set up a next-hop action on a subscriber's interface that forwards traffic to the redirect engine. In this case, you would set the next-hop address to the address of the redirect server.

When you set up redirect server redundancy, both the active and redundant redirect servers share a virtual IP address so that subscribers can always reach the active redirect server. Subscribers send requests to the virtual IP address, and the router automatically sends the request to the active redirect server by means of a static route. In this case, you would set the next-hop address to the virtual IP address.

Configuring Next-Hop Action

To configure a next-hop action:

1. In the side pane, select a JUNOS filters or JUNOSe policy rules.
2. From the Create new list, select **Next Hop**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Interface Actions

Use this action to forward packets to a particular interface and/or a next-hop address. You can configure next-interface actions for JUNOS filters and JUNOSe policy rules. On JUNOSe routers, you can use this action for both ingress and egress parts of the interface.

To configure a next-interface action:

1. In the side pane, select a JUNOS filter or JUNOSe policy rule.
2. From the Create new list, select **Next Interface**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Rule Actions

You can configure next-rule actions for JUNOS filter policy rules. If a packet matches the classify-traffic condition, the next-rule action causes the router to continue to the next rule in the policy list for evaluation.

To configure a next-rule action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Next Rule**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policer Actions

The policer action specifies rate and burst size limits and the action taken if a packet exceeds those limits. You can create policer actions in JUNOS policer and JUNOS filter policy rules.

Each policer action has a packet action. The packet action specifies the action taken on a packet that exceeds its rate limits. You configure packet actions within policer actions. There are four types of actions that you can configure:

- Filter—Packets are discarded.
- Forwarding class—Packets are assigned to the forwarding class that you specify.
- Loss priority—Packets are assigned the loss priority that you specify.
- Parameter—The action specified by the parameter is applied. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

To configure a policer action:

1. In the side pane, select a JUNOS policer or JUNOS filter policy rule.
2. From the Create new list, select **Policer**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. From the Create new list for the policer action, select **Packet Action**. Type a name for the action, and click **OK**.
5. Expand the packet action, and click on the type of packet action that you want to configure for this policer action.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring QoS Profile Attachment Actions

Use this action to specify the name of the QoS profile to attach to the router interface when this action is taken. You can configure QoS actions for JUNOSe policy rules.

The router allows only one QoS profile to be attached to an interface at one time. Therefore, as a subscriber activates and deactivates different services, the QoS profile running on the interface needs to change. The SRC software provides a QoS-tracking plug-in (QTP) that you can use to ensure that as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface. See c.

To configure a QoS profile attachment action:

1. In the side pane, select a JUNOSe policy rule.
2. From the Create new list, select **Qos Attach**. Type a name for the QoS profile attachment action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Rate-Limit Actions

Use this action to define the quality of service. You can configure rate-limit actions for JUNOSe policy rules.

To configure a rate-limit action:

1. In the side pane, select a JUNOSe policy rule.
2. From the Create new list, select **Rate Limit**. Type a name for the rate-limit action, and click **OK**.
3. From the **Type** list, select the type of rate-limit action, either one_rate or two_rate, and click **Apply**.

   The screen changes to display the parameters that you can configure for the type of rate-limit action that you selected.

Configuring Actions for Rate-Limit Actions

Under the rate-limit action, there are three types of actions that you can configure:

- Committed action—Takes action on traffic flows that do not exceed the committed rate.
- Conformed action—Takes action on traffic flows that exceed the committed rate but remain below the peak rate.
- Exceed action—Takes action on traffic flows that exceed the peak rate.

For each committed, conformed, and exceed action, you can select one action to configure—filter, forward, mark, or parameter.

To configure an action for rate-limit actions:

1. Expand the rate-limit action, and expand the action that you want to configure.

1. To set an action to filter, in the side pane select **Filter**, and then click **Create** in the main pane.
2. To set an action to forward, in the side pane select **Forward**, and then click **Create** in the main pane.
3. To set an action to mark:

a. In the side pane, expand **Mark** and select **Mark Info**.

b. In the main pane, click **Create**.

c. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

4. To set an action to parameter:

a. Make sure that you have a packetOperation parameter configured.

b. In the side pane, select **Parameter**, and then click **Create** in the main pane.

c. In the **Action** list, select a parameter.

d. Click **Apply**.

Configuring Reject Actions

You can configure reject actions for JUNOS filter policy rules. The reject action causes the router to discard a packet and send an ICMP destination unreachable message.

To configure a reject action:

1. In the side pane, select a JUNOS filter policy rule.

2. From the Create new list, select **Reject**. Type a name for the action, and click **OK**.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Routing Instance Actions

You can configure routing instance actions for JUNOS filter policy rules. Use routing instance actions for filter-based forwarding to direct traffic to a specific routing instance configured on the router.

To configure a routing instance action:

1. In the side pane, select a JUNOS filter policy rule.

2. From the Create new list, select **Routing Instance**. Type a name for the action, and click **OK**.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Scheduler Actions

You use scheduler actions along with QoS conditions and traffic-shape actions to configure transmission scheduling and rate control. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and random early detection (RED) drop profiles to be applied to a particular class of traffic. You can create scheduler actions in JUNOS scheduler policy rules.

To configure a scheduler action:

1. In the side pane, select a JUNOS schedule policy rule.
2. From the Create new list, select **Scheduler Action**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Drop Profiles

You configure drop profiles within scheduler actions. Drop profiles support the RED process by defining the drop probabilities across the range of delay-buffer occupancy. For a packet to be dropped, it must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet. Depending on the drop probabilities, RED might drop packets aggressively long before the buffer becomes full, or it might drop only a few packets even if the buffer is almost full.

In drop profiles you configure the queue threshold and drop probability as paired values. The values can be either percentage values (segmented) or data points (interpolated). These two alternatives enable you to configure each drop probability at up to 64 fill-level/drop-probability paired values, or to configure a profile represented as a series of line segments. For more information about configuring fill level and drop probabilities, see the JUNOS routing platform documentation.

To configure drop profiles:

1. In the side pane, select a scheduler action.
2. From the Create new list, select **Drop Profile**. Type a name for the drop profile, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Service Class Name Actions

You can configure service class name actions for PCMM policy rules.

To configure a service class name action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select **Service Class Name**. Type a name for the action, and click **OK**.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Stateful Firewall Actions

You can configure stateful firewall actions for JUNOS ASP policy rules. Stateful firewall actions specify the action to take on packets that match the classify-traffic condition.

1. In the side pane, select a JUNOS ASP policy rule.
2. From the Create new list, select **Stateful Firewalls**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. Expand the policy list and expand **Packet Action**.

   A list of actions that can be taken on a packet appears in the side pane. You can configure one type of action.
5. Select the action that you want to configure for the stateful firewall, and click **Create**.
6. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Class Actions

Use this action to put packets in a particular traffic class. You can configure traffic-class actions for JUNOSe policy rules.

To configure a traffic-class action:

1. In the side pane, select a JUNOSe policy rule.
2. From the Create new list, select **Traffic Class**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Mirror Actions

Use this action to mirror traffic from a destination to a source or from a source to a destination. You can configure traffic-mirror actions for JUNOS filter input policy rules.

Before you use traffic-mirror actions, you must configure forwarding options on JUNOS routing platforms for port mirroring and next-hop group. For information about how these features work on the router, see the *JUNOS Policy Framework Configuration Guide*.

The rule containing a traffic-mirror action must comply with these conditions:

- It must be combined with forward actions in the same rule. One of the forward actions must accept the traffic if the source and/or destination IP addresses do not match the conditions.
- It contains either no classify-traffic condition or only one classify-traffic condition.
- It can be marked for accounting.

To configure a traffic-mirror action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Traffic Mirror**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Shape Actions

Traffic-shape actions specify the maximum rate of traffic transmitted on an interface. You can create traffic-shape actions in JUNOS shaping policy rules.

To configure a traffic-shape action:

1. In the side pane, select a JUNOS shaping policy rule.
2. From the Create new list, select **Traffic Shape**. Type a name for the action, and click **OK**.
3. To create a new value for the Rate parameter, enter a value in the box, and click **Add**.
4. Enter information as described in the Help text in the main pane, and click **Apply**.