Chapter 17
Reviewing and Configuring Policies and Services for Enterprise Manager Portal

This chapter provides a high-level overview of the tasks to provision services that service providers make available through Enterprise Manager Portal application. The chapter contains the following sections:

- Overview of Services for Enterprise Manager Portal on page 275

- Before You Configure Services for Enterprise Manager Portal on page 277

- Configuring Firewall Policies and Services for Enterprise Manager Portal on page 277

- Configuring NAT Policies and Services for Enterprise Manager Portal on page 286

- Configuring Bandwidth Policies and Services for Enterprise Manager Portal on page 288

- Enabling Schedules for Subscriptions for Enterprise Manager Portal on page 296

- Configuring VPNs for Enterprise Manager Portal on page 296

- Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms on page 298

Overview of Services for Enterprise Manager Portal

Enterprise Manager Portal is an application that lets service providers provision services for enterprise subscribers. For more information about Enterprise Service Manager, see *Chapter 24, Managing Services with Enterprise Manager Portal*.

Enterprise Manager Portal can apply the types of services listed in Table 23 to enterprise traffic as specified on JUNOS routing platforms or JUNOSe routers.

Table 23: Services Available from Enterprise Manager Portal

Types of Service	Types of Router
Firewalls—stateful or stateless	JUNOS routing platforms
Network Address Translation (NAT)	JUNOS routing platforms
Bandwidth on demand (BoD)	JUNOS routing platforms or JUNOSe routers
BoD for traffic routed to specified layer 3 VPNs	JUNOS routing platforms

The service provider uses services and policies in the SRC directory to manage traffic on a JUNOS routing platform or on a JUNOSe router. IT managers in enterprises that are customers of the service provider subscribe to these services through Enterprise Manager Portal.

Some of the services and policies are defined in the sample data and require little or no customization. You can, however, create some new services and policies, such as those for BoD.

Directory Structure

Use the directory structure in the sample data to organize services and policies. The following list shows the location of the policies and services in the directory:

- Services—*l = entJunos, o = Scopes, o = umc*

- Policies—*ou = entJunos, o = Policies, o = umc*

Although the scope that includes services for Enterprise Manager Portal is named entJunos, the policies for the BoD services have policy rules for both JUNOSe routers as well as JUNOS routing platforms.

Priorities for Subscriptions

Each subscription to a service has a priority that is identified by a service parameter named priority. A subscription with a lower priority setting takes precedence over a subscription with a higher priority setting. The SAE uses the priorities to determine the order in which it applies subscriptions to a particular type of service to traffic. For example, if the same traffic is affected by subscriptions to several firewall services on a JUNOS routing platform, the SAE applies those subscriptions in a prioritized order. Priorities of different types of service are independent of each other; for example, for JUNOS routing platforms, priorities of NAT services are independent of priorities for BoD services.

Depending on the type of service, you must specify either an explicit priority or a range of priorities in the service or the policy rules. When you specify a range of priorities, the IT manager selects an explicit priority in this range through Enterprise Manager Portal. The sample data includes definitions of priorities for each type of service; however, you can modify the priorities if you want to provide different ranges of priorities.

A substitution in a subscription provides the value for the service parameter named priority. This parameter is in the precedence policy rule field to control the ordering of policies when a subscription is activated.

Before You Configure Services for Enterprise Manager Portal

Before you configure services for use by Enterprise Manager Portal:

1. Install the SRC software, and configure the SAE (see *SRC-PE Getting Started Guide, Chapter 33, Installing the SRC Software on a Solaris Platform* and *SRC-PE Getting Started Guide, Chapter 35, Setting Up an SAE on a Solaris Platform*).

2. If you are managing services on JUNOS routing platforms, configure the JUNOS routing platform, and enable it to interact with the SRC software (see the JUNOS documentation set and *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*).

3. If you are managing services on JUNOSe routers, configure the JUNOSe router, and enable it to interact with the SRC software (see the JUNOSe documentation set and *SRC-PE Network Guide, Chapter 5, Using JUNOSe Routers in the SRC Network with the SRC CLI* or *SRC-PE Network Guide, Chapter 6, Using JUNOSe Routers in the SRC Network with a Solaris Platform*).

4. Install the sample data (see *SRC-PE Getting Started Guide, Chapter 34, Defining an Initial Configuration on a Solaris Platform*).

5. For prerequisites to using policy rules on JUNOS routing platforms and JUNOSe routers, see *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

6. For general information about configuring services, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Configuring Firewall Policies and Services for Enterprise Manager Portal

The SRC software represents a JUNOS firewall as two types of SRC services:

■   Basic firewall service—Defines the action that the firewall takes and specifies the types of traffic that the firewall affects.

■   Services to provide firewall exceptions—Defines exception rules to block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which packets and application flows are inspected.

For example, to configure an access only to accept e-mail from a specific IP address, you can use a basic firewall service that blocks all incoming and outgoing traffic; then you can use a firewall exception that allows incoming e-mail traffic from that IP address.

The SRC software supports the following types of firewalls on JUNOS routing platforms:

■ Stateless firewalls—Inspect each packet in isolation; do not evaluate the traffic flow.

■ Stateful firewalls—Inspect track traffic flows and conversations between applications, and evaluate this information when applying exception rules to the traffic.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start.

The same criteria may not be applied to each packet. For example for a TCP application, the criteria changes when a new TCP session is initiated to allow subsequent packets in the flow.

You can make either stateless firewalls or stateful firewalls available from Enterprise Manager Portal.

Overview of Basic Firewall Services and Policies

You can create as many basic firewall services in the directory as you want. Table 24 shows the names of the services and policies associated with the basic firewall services in the sample data.

Table 24: Basic Firewall Services and Policies

Name of Service	Name of Policy Group	Function of Firewall
BrickWall	brickwall	Blocks all incoming and outgoing traffic
EmailAndWeb	emailweb	Blocks all incoming traffic and allows only outgoing e-mail and HTTP traffic
Multiservice	multiservice	Blocks all incoming traffic and allows outgoing e-mail, HTTP, FTP, telnet, and Real-Time Streaming Protocol (RTSP) traffic

The services are located under $l = entJunos, o = Scopes, o = umc$ in the sample data.

The policies are located under $ou = entJunos, o = Policies, o = umc$ in the sample data.

You can use these services and their associated policies as a starting point for developing your own basic firewall services.

Tasks to Configure Firewall Policies and Services

The tasks to configure policies and services for firewalls are:

1. Configuring Basic Firewall Policies on page 279

2. Configuring Basic Firewall Services on page 280

3. For stateful firewalls:

   a. Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls on page 280

   b. Reviewing the FirewallRule Service for Exceptions to Stateful Firewalls on page 280

4. For stateless firewalls:

   a. Reviewing Services for Exceptions to Stateless Firewalls on page 281

   b. Parameter Values Used by Services for Exceptions to Stateless Firewalls on page 282

   c. Planning Services for Custom Firewall Exceptions on page 282

   d. Configuring Policies for Custom Firewall Exceptions on page 283

   e. Configuring Services for Custom Firewall Exceptions on page 284

Configuring Basic Firewall Policies

You can create policies from Policy Editor. For information about creating firewall policies, including prerequisites on the JUNOS routing platform, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To create a basic firewall policy:

1. Create a policy group and associated policy rules in *ou = entjunos, o = Policies, o = umc*.

2. Specify a precedence for the policy rules.

   All basic firewall services should have a similar value that is higher than the range of precedences you configure for firewall exceptions. In the sample data, we use precedences of 600 and 601 for basic firewall policies.

   Ensure that the precedence for basic firewall policies integrate with other policies that affect the same traffic. See *Configuring Priorities for Stateless or Stateful Firewall Services* on page 284.

For a sample basic firewall policy, see *policyGroupName = brickwall, ou = entjunos, o = Policies, o = umc* in the sample data.

Configuring Basic Firewall Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To create a basic firewall service:

1. Create a service.

2. Specify the following values for the service:

    ■   Category—Text string basicFirewall (service's LDAP attribute sspCategory)

    ■   Description—Summary of what the firewall service does (service's LDAP attribute description)

        This description will appear on the portal, and subscribers will use the description to select a firewall service. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

    ■   Policy Group—Policy group configured for use with this service

For a sample firewall service, see *serviceName = BrickWall, l = entJunos, o = Scopes, o = umc* in the sample data.

Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls

The policy group *policyGroupName = fwrule, ou = entJunos, o = Policies, o = umc* is predefined in the sample data. Do not modify any settings or substitutions for this service.

Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls

The SRC sample data provides one service for firewall exceptions, *serviceName = FirewallRule, l = entJunos, o = Scopes, o = umc,* that is designed to work with Enterprise Manager Portal. Do not modify the definition for this service or its associated policy.

You can modify the allowed priority ranges for the service. See *Configuring Priorities for Stateless or Stateful Firewall Services* on page 284.

Each subscription to this service adds a rule to the stateful firewall. The FirewallRule service and its associated policy are general and contain many parameters, such as the priority of the firewall exception and the action that the firewall should take. IT managers supply actual values for these parameters through Enterprise Manager Portal.

You can modify the priority ranges for this policy group if necessary; do not modify any other settings. The values for these parameters must be lower than the precedence settings for the policy rules in the basic firewall policy groups. This distinction allows the firewall exception to take priority over the basic firewalls. In the sample data, the FirewallRule service has priorities in the range 500–579.

Reviewing Services for Exceptions to Stateless Firewalls

Review the services that Enterprise Manager Portal requires to ensure that configuration of these services works in your environment. These services are firewall exceptions—services that define the types of traffic that a firewall admits or blocks.

Enterprise Manager Portal requires that specific services be configured to cover each of the following traffic actions:

■ Allow

■ Reject

■ Discard

These actions are required for each traffic direction; that is, traffic:

■ Entering the network

■ Exiting the network

■ Entering and exiting the network

Table 25 lists the names of services required by Enterprise Manager Portal. The naming convention for the services specifies both action and direction; for example, for the FWR_Fwd_Out service:

■ Action—allow (forward)

■ Direction—Outgoing (from the enterprise)

Services configured to reject traffic return a "network-unreachable" ICMP message.

Table 25: Stateless Firewall Services in Sample Data

	Traffic Entering the Enterprise	**Traffic Exiting from the Enterprise**	**Traffic Entering and Exiting the Enterprise**
Traffic Allowed	FWR_Fwd_In	FWR_Fwd_Out	FWR_Fwd_Both
Traffic to Be Discarded	FWR_Filter_In	FWR_Filter_Out	FWR_Filter_Both
Traffic Rejected	FWR_Rej_In	FWR_Rej_Out	FWR_Rej_Both

The services are located under *l = entJunosStatelessFW, o = Scopes, o = umc* in the sample data. These services and the associated policies configured in the sample data are designed for a subscriber–facing interface on a provider edge device.

In most cases you can use the services as configured. If needed—for example, for a service provider–facing interface in a customer edge device—you can customize the services listed in Table 25, but do not change the names.

To customize services for an enterprise-facing interface, change the configuration for:

■ Source IP addresses and ports

■ Destination IP addresses and ports

You can also create services that provide custom exceptions to a firewall. Portal users can select custom exceptions under Firewall actions on the Firewall page in Enterprise Manager Portal.

Parameter Values Used by Services for Exceptions to Stateless Firewalls

Table 26 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with "fw" (service's LDAP attribute parameterSubstitution). The services listed in *Before You Configure Services for Enterprise Manager Portal* on page 277 use these parameters.

Table 26: Parameters for Stateless Firewall Services for Enterprise Manager Portal

To Specify this Value	Use This Parameter
Protocol	fwProtocol
Source network	fwSrcIp
Source port	fwSrcPort
Destination network	fwDestIp
Destination port	fwDestPort
TOS byte	fwTosByte
TOS byte mask	fwTosByteMask
TCP flags	fwTcpFlags
TCP flags mask	fwTcpFlagsMask
IP flags	fwIpFlags
IP flags mask	fwIpFlagsMask
Fragmentation offset	fwIpFragOffset
ICMP type	fwIcmpType
ICMP code	fwIcmpCode
Packet length	fwPacketLength

Planning Services for Custom Firewall Exceptions

Typically, you use custom exceptions to provide bandwidth management as well as firewall exceptions. Using custom exceptions that do both simplifies the way you integrate BoD and firewall services. For example, you can create custom exceptions to police traffic or to assign a traffic class to the traffic and to specify firewall behavior.

See examples of services for custom exceptions in the sample data:

■ *l = Limit1Mbs, l = entJunosStatelessFW, o = Scopes, o = umc*

■ *l = Limit2Mbs, l = entJunosStatelessFW, o = Scopes, o = umc*

■ *l = Limit5kbs, l = entJunosStatelessFW, o = Scopes, o = umc*

The sample services and the associated policies are designed for a subscriber–facing interface on a provider edge device. When you create policies, policy direction (input or output) can map to incoming or outgoing traffic depending on whether the SRC-managed interface is a subscriber–facing interface on a service provider edge device, or a service–provider facing interface on the customer edge device in an enterprise. When you configure policies for services designed for use through the Enterprise Management Portal, you typically assume that:

■ Source IP addresses and ports are inside an enterprise

■ Destination IP addresses and ports are outside an enterprise

Configuring Policies for Custom Firewall Exceptions

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*. For information about managing policies, see *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

To configure a policy for a custom firewall exception:

1. Create a stateless firewall policy group and associated policy rules.

2. Specify parameters for the following properties for each policy rule:

    ■ IP protocol

    ■ TOS byte in the IP header

    ■ Source IP addresses

    ■ Source TCP/UDP ports

    ■ Destination IP addresses

    ■ Destination TCP/UDP ports

    ■ TCP flags

    ■ IP flags (fragmentation flags)

    ■ Fragmentation offset

    ■ Packet length

- ICMP type

- ICMP code

For a sample policy, see *policyGroupName = custom_policer,*
ou = entjunos_statelessfw, o = Policies, o = umc in the sample data.

Configuring Services for Custom Firewall Exceptions

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 5, Scheduling Services on a Solaris Platform*. You can create services that take actions such as those listed in Table 25.

To configure a service for a custom firewall exception:

1. Create a service for each traffic action listed in Table 25. Specify a name that provides meaningful information to a user, including information about the forwarding treatment for traffic. The name appears in the Firewall Action field on the Firewall tab in Enterprise Manager Portal.

2. Specify the following values for the service:

   - Category—customFWRule (the service's LDAP attribute sspCategory)

   - Policy Group—Policy group that supports custom firewall exceptions

3. Specify substitutions for the service.

Configuring Priorities for Stateless or Stateful Firewall Services

If you design services to be accessed from Enterprise Manager Portal, you can configure ranges of priority values that are enterprise specific and ranges that are available to a number of enterprises. Setting the two ranges makes it possible for a service provider to specify firewall exceptions that an IT manager in an enterprise cannot override.

Configuring Priorities to Have Enterprise Services Work Together

You can configure the parameters in the following list as global parameters that apply to all subscribers, and as subscriber-specific parameters. If you configure both, the global range takes precedence over a subscriber-specific limit.

- fwMinPriority—Specifies the lower limit of the range of precedences available for subscriptions to firewall exceptions.

- fwMaxPriority—Specifies the upper limit of the range of precedences available for subscriptions to firewall exceptions.

- fwEnterpriseMinPriority—Specifies the lower limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

- fwEnterpriseMaxPriority—Specifies the upper limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

Ensure that:

- fwMaxPriority is greater than or equal to fwEnterpriseMaxPriority

- fwEnterpriseMaxPriority is greater than fwEnterpriseMinPriority

- fwEnterpriseMinPriority is greater than or equal to fwMinPriority

Configuring Global Priority Ranges from Policy Editor

Before you configure the global priority range, make sure that the sample data for Enterprise Manager Portal is loaded. If the sample data is not available, you must create a parameter similar to fwEnterpriseMinPriority.

To configure priorities for firewall policy rules from Policy Editor:

1. In Policy Editor, in the navigation pane select **Parameters**.

2. Under Parameters, select a priority, such as fwEnterpriseMinPriority, and on the General tab change the value for Default Value.

Configuring Global Priority Ranges from SDX Admin

Before you configure the global priority range, make sure that the sample data for Enterprise Manager Portal is loaded. If the sample data is not available, you must create a parameter similar to fwEnterpriseMinPriority in Policy Editor.

To configure priorities for firewall services from SDX Admin:

1. In SDX Admin, in the navigation pane select **Parameters**.

2. Under Parameters, select a priority, such as fwEnterpriseMinPriority, and on the Main tab change the value for Default Value.

Configuring Priorities for Individual Scopes by Defining Them in Services

You can use parameters to limit priority ranges for services within a scope. For stateful firewall services, you set parameters to limit priority ranges in the FirewallRule service. For stateless firewall services, you set parameters to limit priority ranges in the FRW_Filter_Both service.

You can use parameters to limit priority ranges for services within a scope in addition to using global ranges. For example, you can define a global range, and then define a different range that overrides the global range for specified subscribers.

To allow priority values for services in one scope to override the priority values for services in another scope:

1. In a service that resides in a service scope that has a low precedence (indicated by a higher number), define default values for parameters that limits a priority range.

2. Attach this scope to an entry at a high level in the subscriber folder; for example, to a retailer.

3. Create a second scope that has a higher precedence.

4. Create a service that uses parameters to limit priority ranges in the second scope.

5. Attach the second scope (which has a higher precedence) to the enterprise.

The services with the higher precedence override the services with a lower precedence.

Using Stateless Firewall and BoD Applications Together

In most cases, you can use the services listed in Table 25 on page 281 to provide bandwidth management and firewall support. However, if you want to design special services to have firewalls work with BoD services, use the following guidelines to design your services:

■ Specify a higher priority in the BoD policies.

■ Specify next–rule actions for the BoD policies.

After all the BoD policy rules are applied, the stateless firewall policy rules are applied. Packets are forwarded or dropped as appropriate.

Configuring NAT Policies and Services for Enterprise Manager Portal

The NAT policy groups and services provided in the sample data are designed to work with Enterprise Manager Portal and require little configuration. Table 27 shows the names of the policy groups and services associated with each type of NAT that the SRC software supports.

Table 27: NAT Services and Policies

Type of NAT	Name of Policy Group	Name of Service
Dynamic source NAT	dynsrcnat	DynSrcNat
Static destination NAT	staticdstnat	StaticDstNat
Static source NAT	staticsrcnat	StaticSrcNat

The services are located under $l = entJunos, o = Scopes, o = umc$ in the sample data.

The policies are located under $ou = entJunos, o = Policies, o = umc$ in the sample data.

For information about creating NAT policies, including prerequisites on the JUNOS routing platform, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Configuring the dynsrcnat Policy Group

You can modify the precedence settings in the policy rules for the dynsrcnat policy group. Use the following guidelines if you make changes to the precedence settings:

- The precedence settings for the policy rules in the dynsrcnat policy group must be higher than the precedence settings for the policy rules in the staticsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

- The value for this setting must be higher than the precedence of any firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Reviewing the DynSrcNat Service

The DynSrcNat service is predefined in the sample data. Do not modify any settings or substitutions for this service.

Configuring the staticdstnat Policy Group

This policy group contains two policy rules:

- SFWR —Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.

- PR—Defines the policy for the static destination NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticDstNat Service

You can modify the following substitutions for the StaticDstNat service; do not modify any other settings for this service.

- staticDestNatMinPriority—Lower limit of the range of precedences available for subscriptions to static destination NAT rules

- staticDestNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static destination NAT rules

Configuring the staticsrcnat Policy Group

This policy group contains two policy rules:

- SFWR—Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.

- PR—Defines the policy for the static source NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticSrcNat Service

You can modify the following substitutions for the StaticSrcNat service; do not modify any other settings or substitutions for this service.

- staticSrcNatMinPriority—Lower limit of the range of precedences available for subscriptions to static source NAT rules

- staticSrcNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static source NAT rules

The values for these parameters must be lower than the precedence settings for the policy rules in the dynsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

Configuring Bandwidth Policies and Services for Enterprise Manager Portal

You can make bandwidth available on demand to IT managers by creating the following types of services:

- Basic BoD service—Specifies the bandwidth level available to an access link.

- BoD service—Classifies traffic and assigns a service level that specifies the forwarding treatment for the traffic class.

BoD and basic BoD services allow billing for subscriptions to supplementary services.

You can create services to provide JUNOS class of service (CoS) or JUNOSe quality of service (QoS) by configuring BoD and basic BoD services that interact with each other. You can provide different service levels to different traffic by specifying traffic classification criteria.

You can create any number of basic BoD services and any number of BoD services. Only one basic BoD service, but numerous BoD services can be assigned to an access link.

BoD services can be configured to provision bandwidth provided by basic BoD services for a link. For example, you could provide a basic BoD service that provides 1 Mbps to the access link, and two video services as BoD services, each with different characteristics.

When you configure BoD and basic BoD services, they are available to IT managers through Enterprise Manager Portal. For information about how IT managers configure BoD and basic BoD services through Enterprise Manager Portal, see *Chapter 23, Managing Enterprise Service Portals*.

Parameter Values Used by BoD Services

Table 28 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with "bod" (service's LDAP attribute parameterSubstitution).

Table 28: Parameters for BoD Services for Enterprise Manager Portal

To Specify This Value	Use This Parameter
Protocol	bodProtocol
TOS byte	bodTosByte
TOS byte mask	bodTosByteMask
Source network	bodSrcIp
Source port	bodSrcPort
Destination network	bodDestIp
Destination port	bodDestPort
TCP flags	bodTcpFlags
TCP flags mask	bodTcpFlagsMask
IP flags	bodIpFlags
IP flags mask	bodIpFlagsMask
Fragmentation offset	bodIpFragOffset
Packet length	bodPacketLength
ICMP type	bodIcmpType
ICMP code	bodIcmpCode

Bandwidth Policies for Different Routing Platforms

If you support environments that include both JUNOSe routers and JUNOS routing platforms, you can configure policies to have policy rules for JUNOSe filters and JUNOS filters. This way, if the service is activated on a JUNOSe router, the JUNOSe rule is used, and if the service is activated on a JUNOS routing platform, the JUNOS policies are used.

When Enterprise Manager Portal has JUNOSe compatibility enabled, the portal allows:

- Single subnets for source and destination addresses

- Single ports or single port ranges for source and destination ports

In addition, with JUNOSe compatibility enabled, Enterprise Manager Portal does not show the following configuration fields for BoD services:

- TCP flags

- IP flags

- Fragment offset

- Packet length

- ICMP type

- ICMP code

You should be familiar with the types of bandwidth management policies available for the type of router for which you are configuring policies. See *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

Configuring Basic BoD Policies

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a basic BoD policy:

1. Create a policy group and associated policy rules.

   Typically the policy rules include JUNOS schedulers, JUNOS policers, JUNOS filters, or JUNOSe filters that specify a traffic classification, and basic rules that define best-effort forwarding and drop behavior.

2. Include parameters in the classify-traffic conditions of the policer. Use parameter names from Table 28 on page 289.

3. Specify a precedence for the policy rules.

   Structure the precedence for policies to ensure that policy rules for JUNOS schedulers and JUNOS policers have a higher precedence, and therefore a lower number, than default policy rules. If the configuration includes BoD services, the policies to support BoD services should have a higher precedence, indicated by a lower number.

For a sample basic BoD policy, see *policyGroupName = basicBod, ou = entjunos, o = Policies, o = umc* in the sample data.

Configuring Basic BoD Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Basic BoD services do not have service parameters.

To configure a service that uses basic BoD:

1. Create a service.

2. Specify the following values for the service:

    ■   Category—basicBod (service's LDAP attribute sspCategory)

    ■   Description—Description of the bandwidth provided by the service

        If you plan to integrate a basic BoD service with a BoD service, the description for each basic BoD service should explain the bandwidth provided, and the relationship between this bandwidth level and the BoD service. The description should also explain the relationship between the service name, which is shown on the portal in the Bandwidth Level list, and the bandwidth provided. For example, for a service named 1 Mbps, the bandwidth provided could be 1 Mbps downstream and 500 Kbps upstream.

        This description will appear in the online help for Bandwidth Level in Enterprise Manager Portal. Although there is no limit for the length of the text entered, the portal displays the text in one paragraph.

    ■   Policy Group—Policy group that supports basic BoD services

For a sample BoD service, see *serviceName = 1.0 Mbps, l = EntJunos, o = Scopes, o = umc* in the sample data.

Configuring BoD Policies

When configuring BoD policies, you create rules that classify traffic. Make sure that the source and destination policy rules correspond to location of the enterprise relative to the subscriber interface that the SRC software manages. When configuring Enterprise Manager Portal, you follow the same rules for defining source and destination fields. See *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a BoD policy:

1. Create a BoD policy group and associated policy rules.

    You can create some policy rules as JUNOS filters and others as JUNOSe filters.

    Specify values or parameters for the following for each policy rule for the BoD service:

    ■   TOS byte in the IP header

- Mask used for the ToS byte

- Source TCP/UDP port

- Destination TCP/UDP port

- IP address of source

- IP address of destination

- TCP flags

- Fragmentation flags

- Fragmentation offset

- ICMP type

- ICMP code

2. Specify a precedence for the policy rules.

   If the configuration includes basic BoD services, the policies to support basic BoD services should have a lower precedence, indicated by a higher number.

   For information about policy rules and precedences, see See *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

For a sample BoD policy, see *policyGroupName = bod, ou = entjunos, o = Policies, o = umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

The sample data is based on a scenario that has the SRC managed interface on a device with egress to the access link that leads to the enterprise.

Configuring BoD Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

NOTE: If you configure BoD services that use forwarding classes, take into consideration the number of forwarding classes supported on the router.

To configure a service for BoD:

1. Create a service.

2. Specify the following values for the service:

   ■ Category—bod (service's LDAP attribute sspCategory).

   ■ Description—Description of how this service will affect traffic.

     If you plan to integrate a basic BoD service with a BoD service, the description for each BoD service should take into consideration how the BoD service interacts with any basic BoD service selected. The description should also provide information about the forwarding treatment for traffic.

     This description will appear in the online help for BoD services in Enterprise Manager Portal. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

   ■ Substitutions—Substitutions for the parameter names; these names start with "bod" (service's LDAP attribute parameterSubstitution).

     Note that the actual parameter names are required to be the service parameter names for Enterprise Manager Portal.

   ■ Policy Group—Policy group that supports BoD services.

For a sample BoD service, see *serviceName = Gold, l = entJunos, o = Scopes, o = umc* in the sample data.

Using BoD Services to Assign Traffic to Bandwidth Categories

You can use BoD services to assign different classes of traffic to different bandwidth categories, with each category identified by a specified quantity of bandwidth.

For example, a configuration could provide two services:

■ Silver—Bandwidth of 500,000 Mbps

■ Gold— Bandwidth of 1,000,000 Mbps

Each service has the specified bandwidth available to specified traffic flows, based on the policy rules for traffic classification and policing.

Using BoD and Basic BoD Services Together to Supply Class of Service

You can use BoD and basic BoD services together to provide more sophisticated bandwidth level management to IT managers. For example, you can integrate these types of services to take advantage of the CoS features available on JUNOS routing platforms.

On the JUNOS routing platform, policers are applied before schedulers. The type of service defined by these settings is applied to traffic exiting from the JUNOS routing platform. For information about policing, scheduling, and queuing traffic on the JUNOS routing platform, see *JUNOS Network Interfaces and Class of Service Configuration Guide*.

If you want to integrate basic BoD services and BoD services, you can base your configuration on the implementation in the sample data, The sample services and data are designed to work with Enterprise Manager Portal and require little configuration.

You can also create a configuration to meet requirements specific to your environment. If you want to create a configuration that has both basic BoD and BoD services, carefully plan services and associated policies. Ensure that the bandwidth requirements for BoD services are in proportion to the bandwidth provided by the basic BoD services. See *Setting Up Forwarding Preferences—Example 2* on page 295 for another way to provide BoD to IT managers.

☞ **NOTE:** When configuring services to use JUNOS CoS, take into consideration which interfaces on the router support CoS.

Setting Up Forwarding Preferences—Example 1

The sample data provides an implementation that supports CoS features on the JUNOS routing platform. This implementation provides:

- Basic BoD services to apply a JUNOS policer only to best-effort traffic

- BoD services to assign traffic to forwarding classes other than best-effort

- Policing for best-effort traffic

Table 29 lists the services and policies in the sample data. You can locate the services in *l = entJunos, o = Scopes, o = umc*. You can customize the policies and services as needed. For general information about configuring policies and services, see *Configuring Basic BoD Policies* on page 290 and *Configuring BoD Policies* on page 291.

Table 29: Integrated BoD and Basic BoD Services in Sample Data

Name of Service	Category of Service	Name of Policy Group	Description of Service
1.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 1.0 Mbps be available to a specified access link for best-effort traffic.
3.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 3.0 Mbps be available to a specified access link for best-effort traffic.
5.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 5.0 Mbps be available to a specified access link for best-effort traffic.

Table 29: Integrated BoD and Basic BoD Services in Sample Data   (continued)

Name of Service	Category of Service	Name of Policy Group	Description of Service
Silver	BoD	BoD	Marks associated traffic as belonging to an assured forwarding class.
Gold	BoD	BoD	Marks associated traffic as belonging to an expedited forwarding class.

Billing can be established for traffic in the assured forwarding class and in the expedited forwarding class because the SRC software can account for traffic in each of these forwarding classes separately from other forwarding classes. Traffic in the assured forwarding class and in the expedited forwarding class is not included in the accounting data for the currently selected basic BoD service.

Setting Up Forwarding Preferences—Example 2

The following example shows another way to use BoD and basic BoD services to provide BoD services. In this example, a percentage of an access link's bandwidth is allocated to a specified service.

This configuration provides:

- Three bandwidth levels available to access links: 1.0 Mbps, 1.5 Mbps, and 2.0 Mbps.

- Three service levels defined to use a specified percentage of the bandwidth set for the access link: best effort 20 %, Silver 30 %, and Gold 50 %.

  Each traffic class uses only the bandwidth assigned to it and does not share bandwidth with other traffic classes.

For an SRC configuration to support this scenario, you could create policies such as the following and assign these policies to services:

- Policies that provide a local policy parameter, bw, whose value is set by the service that references the policy:

  For policy 1.0 Mb, bw = 1000000

  For policy 1.5 Mb, bw = 1500000

  For policy 2.0 Mb, bw = 2000000

- The transmission rate, bandwidth allocation, and priority scheduling for specified forwarding classes as shown in Table 30.

Table 30: Policies to Specify Forwarding Treatment for Specified Traffic Classes

Forwarding Class	Transmission Rate	Exact	Priority Scheduling
Best effort	bw*0.2 bps	true	Low
Silver (assured forwarding)	bw*0.3 bps	true	Medium
Gold (expedited forwarding)	bw*0.5 bps	true	High

By setting exact to true, you can ensure that the sum of the transmission rates is less than the bandwidth allocated to the access link.

Enabling Schedules for Subscriptions for Enterprise Manager Portal

You can add schedules to subscriptions from Enterprise Manager Portal for subscriptions to BoD and firewall services that have scheduling enabled. To enable scheduling:

1. In SDX Admin, select the service to be scheduling-enabled.

2. In the Parameter tab, add the Substitution **isSchedulable = 1**.

   This substitution lets enterprise subscribers configure schedules for subscribers to this service.

Configuring VPNs for Enterprise Manager Portal

You can use the SRC software to allow IT managers to manage layer 3 VPNs on JUNOS routing platforms. This type of VPN supports membership based on filter-based forwarding policies.

You can configure Enterprise Manager Portal to display VPN features. IT managers can modify VPNs and send traffic associated with BoD subscriptions to specific VPNs. In addition, if you configure Enterprise Manager Portal to display extranet features, IT managers with privileges to configure VPNs can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To provide VPN services from Enterprise Manager Portal, you create corresponding VPN versions of the BoD services and their associated policies.

Before You Configure VPN Policies and Services

When you configure the SRC software to manage VPNs, you must perform some additional tasks to those listed in *Before You Configure Services for Enterprise Manager Portal* on page 277:

1. Configure the VPNs on the JUNOS routing platform (see *JUNOS VPNs Configuration Guide)*.

   All routing instances that implement a specific VPN must have the same name.

2. Add the VPNs to the directory (see *Chapter 19, Adding VPNs from JUNOS Routing Platforms*).

   The identifier for a VPN in the directory must match the name of the routing instance configured on the JUNOS routing platform (see Step 1).

3. If you want to send traffic associated with BoD services to specific VPNs, configure policies and services for BoD traffic destined for VPNs (see *Configuring Policies for BoD Traffic Destined for VPNs* on page 297 *and Configuring Services for BoD Traffic Destined for VPNs* on page 298).

4. Implement an addressing scheme for VPNs that allows extranet clients to access the VPNs (see *Implementing a Routing Scheme for VPNs* on page 308).

Configuring Policies for BoD Traffic Destined for VPNs

You can manage policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a policy for a BoD service associated with a VPN (a VPN policy):

1. Copy the policy for the BoD service in the directory.

2. Rename the policy you copied to a similar name that indicates this policy is the VPN version; for example, you can use < bodPolicy > Vpn, where < bodPolicy > is the name of the BoD policy.

   For example, if the name of the original policy is bod, rename the service you copied to bodVpn.

3. Add a new local parameter (the name is arbitrary, for example vpnName) of type Routing Instance to the VPN policy.

4. Add a new action of type RoutingInstanceAction to the input policy rule, and specify a Routing Instance of vpnName for this action.

5. Save the VPN policy.

For a sample VPN policy, see *policyGroupName = bodVpn, ou = entjunos, o = Policies, o = umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

Configuring Services for BoD Traffic Destined for VPNs

You can manage services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform.*

To configure a BoD service that will be associated with a VPN (a VPN service):

1. Copy the BoD service in the directory.

2. Rename the service you copied to < bodService > _VPN, where < bodService > is the name of the original BoD service.

    For example, if the name of the original BoD service is called Gold, rename the service you copied to Gold_VPN.

3. Add to the VPN service a parameter with a name that matches the parameter of type Routing Instance that you defined in the policy (see Step 3 of *Configuring Policies for BoD Traffic Destined for VPNs* on page 297).

    !vpnName=bodVpnName

4. Modify the VPN service to use the corresponding VPN policy that you created.

5. Save the service.

For a sample VPN service, see *serviceName = Gold_VPN, l = entJunos, o = Scopes, o = umc* in the sample data.

Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms

All services that you configure for JUNOS routing platforms support billing that uses the source class usage (SCU) and destination class usage (DCU) features for egress traffic on the JUNOS routing platform. The SRC software supports this feature through the SAE and policy engine, which match source and destination classes in JUNOS policy rules. To enable SCU/DCU-based billing:

1. Configure the JUNOS routing platforms in the network to support SCU/DCU accounting, ensuring that all traffic is tagged with the appropriate classes.

    The classes depend on the routes that the routers use to forward the traffic. For information about configuring SCU/DCU accounting with the JUNOS software, see the JUNOS documentation set.

2. Configure policies that match the source and destination classes you defined and that contain accounting rules.

3. Configure the services to which enterprises subscribe to use these policies.

For example, a service provider may want to bill local and long-distance traffic at different rates. The service provider could achieve this goal as follows:

1. Configure the JUNOS routing platform to tag traffic that exits the SRC network with the class netout and traffic that stays within the network with the class netin.

2. Define a service called LocalBestEffortData, and associate with this service a policy that matches the destination class netin at output.

3. Define a service called LongDistanceBestEffortData, and associate with this service a policy that matches the destination class netout at input and output.

The service provider can monitor the use of each service and whether the traffic remains within the network. With this information, the service provider can bill the enterprise accordingly. An IT manager in the enterprise can subscribe to both services and can monitor the enterprise's use of each service through the portal.