Chapter 13

Policy Examples Created with Policy Editor

This chapter gives examples of policies that service providers can use to provide Internet access and to deploy different types of services. The examples in this chapter are created with Policy Editor. To see these examples created with the SRC CLI, see *Chapter 12, Policy Examples Created with the SRC CLI*.

Topics in this chapter include:

Example: Creating Access Policies for Subscribers

In this example, the service provider manages an interface on the router. The interface is associated with a subscriber. The access policy is a default policy that supports various types of subscribers and interfaces. Some examples are DHCP, static IP subscribers, and PPP subscribers.

The default policy installed on the interface sets the context of other services that the subscriber will activate later. The default policy can restrict subscriber access to the network or provide a default access. You can also use the default policy to create a walled garden effect by sending subscribers to the SSP server and requiring them to activate a service before they can access other services in the system. (The term walled garden is used to describe an environment in which a service provider limits a subscriber's access to Web content and services.)

The precedence of the policy rules in default policies is very important. When the related service is activated, the service policy needs a high priority (low value) so that the service policy is used instead of the default policy.

Types of Policies

The policy used for access depends on the type of services that it will be used for. Generally, policies with filter, forward, rate-limit or policer, and next-hop actions are used.

Sample Access Policies

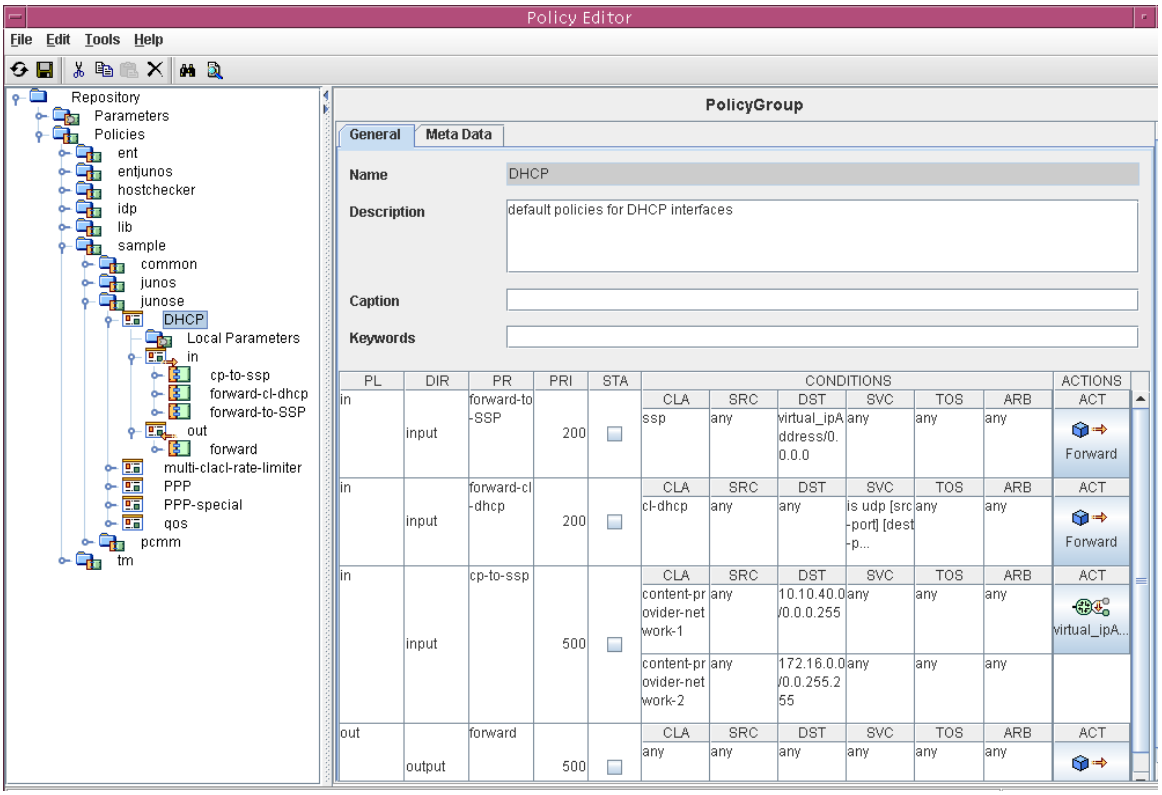
This section contains examples of access policies for DHCP subscribers and PPP subscribers. In both of these examples, there are two content providers. Traffic destined for the content provider networks is sent to the residential portal by using a next-hop action that forwards traffic to the virtual IP address of the SSP. (See *SRC-PE Sample Applications Guide*.)

Traffic to the SSP has a high priority and is not affected by other service policies. This way, the subscriber can always access the SSP. Traffic from the network is forwarded without any restrictions.

DHCP Policy Group

Figure 32 shows a summary of the access policy for DHCP subscribers.

Figure 32: DHCP Policy Group



The following information shows the configuration details of the DHCP policy group in Figure 32.

policyGroupName=DHCP, ou=junose, ou=sample, o=Policies, o=umc

PolicyList out

```
       name=out
       policyRoles=JUNOSE
       applicability=output

   PolicyRule forward
        priority=500
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition
     Forward Action
```

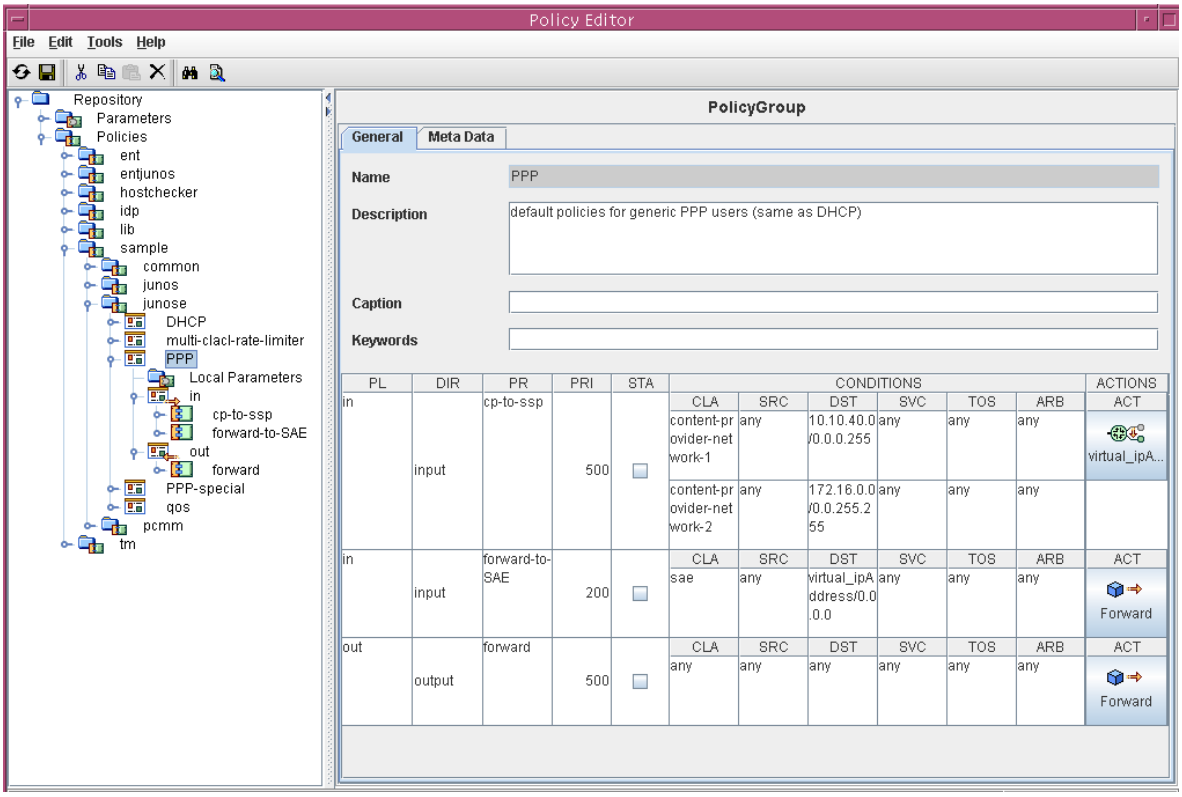
PolicyList in

```
       name=in
       policyRoles=JUNOSE
       applicability=input

   PolicyRule cp-to-ssp
        priority=500
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition content-provider-network-1
        DestinationNetwork:
          ipAddress=10.20.40.0
          ipMask=255.255.255.0
          ipOperation=is
     ClassifyTrafficCondition content-provider-network-2
        DestinationNetwork:
          ipAddress=172.16.0.0
          ipMask=0.0.255.255
          ipOperation=is
     NextHop Action
        nextHopAddress=virtual_ipAddress

   PolicyRule forward-cl-dhcp
        priority=200
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition
        protocol=udp
        DestinationNetwork:
          ipAddress=0.0.0.0
          destination port=67
     Forward Action

   PolicyRule forward-to-ssp
        priority=200
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition
        DestinationNetwork:
          ipAddress=virtual_ipAddress
          ipMask=255.255.255.255
          ipOperation=is
     Forward Action
```

PPP Policy Group

Figure 33 shows a summary of the access policy for PPP subscribers.

Figure 33: PPP Policy Group



The following information shows the configuration details of the PPP policy group in Figure 33.

policyGroupName=PPP, ou=junose, ou=sample, o=Policies, o=umc

PolicyList out

```
        name=out
        policyRoles=JUNOSE
        applicability=output

   PolicyRule: name=forward
        priority=500
        type=JUNOSE
        accountingRule=false
     Forward Action
```

PolicyList in

```
        name=in
        policyRoles=JUNOSE
        applicability=input

   PolicyRule: name=cp-to-ssp
        priority=500
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition content-provider-network-1
        DestinationNetwork:
          ipAddress=10.10.40.0
          ipMask=255.255.255.0
          ipOperation=is
     ClassifyTrafficCondition content-provider-network-2
        DestinationNetwork:
          ipAddress=172.16.0.0
          ipMask=255.255.0.0
          ipOperation=is
     NextHop Action
        nextHopAddress=virtual_ipAddress

   PolicyRule: name=forward-to-ssp
        priority=200
        type=JUNOSE
        accountingRule=false
     ClassifyTrafficCondition sae
        DestinationNetwork:
          ipAddress=virtual_ipAddress
          ipMask=255.255.255.255
          ipOperation=is
     Forward Action
```

Example: Providing Tiered Internet Services with Policing

In this scenario, the service provider offers three tiered Internet services to its subscribers:

- Gold, which provides a bandwidth of up to 5 Mbps.
- Silver, which provides a bandwidth of up to 1Mbps.
- Bronze, which provides a bandwidth of up to 64 Kbps.

One of the tiered Internet services controls the traffic at a given time. Accounting data is collected for the tiered services.

A default policy is needed to establish the context of the tiered service. The subscriber has an IP interface in the network; the access point has a default policy that prevents the subscriber from using a tiered Internet service until the service is activated.

Types of Policies

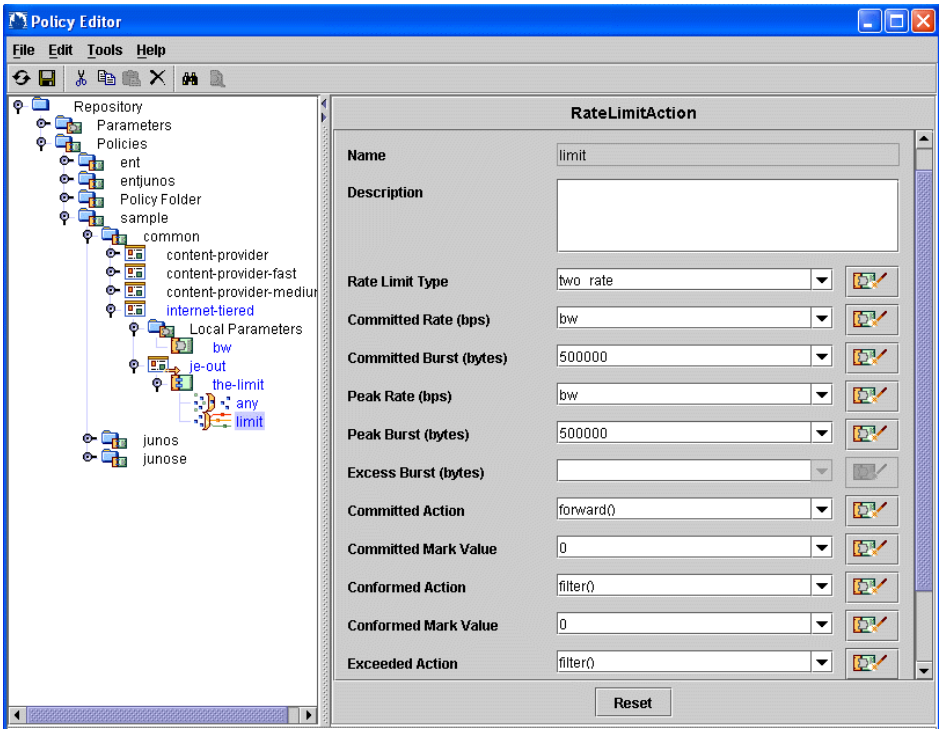
JUNOSe policies use the rate-limit action to control bandwidth, and JUNOS policies use the policer action to control bandwidth. You could also use QoS conditions and scheduler actions to provide tiered Internet services.

Sample JUNOSe Rate-Limiting Policy

The sample JUNOSe policy has a local parameter bw, which is used in the rate-limit action both on input and output directions.

In this example, the committed action is forward, whereas the conformed and exceeded actions are set to filter.

Figure 34: Rate-Limit Action for Tiered Internet Service



The following information shows the configuration details of the Internet tiered policy group for JUNOSe routers.

policyGroupName=internet-tiered, ou=common, ou=sample, o=Policies, o=umc

Local Parameter

```
name=bw, defaultValue=5000000, parameterType=rate
```

PolicyList je-out

```
        name=je-out
        policyRoles=JUNOSE
        applicability=output

PolicyRule: name=the-limit
        priority=600
        type=JUNOSE
        accountingRule=true
     ClassifyTrafficCondition
     RateLimit Action
        rateLimitType=two_rate
        committedRate=bw
        committedBurst=500000
        peakRate=bw
        peakBurst=500000
        committed=Forward
        conformed=Filter
        exceeded=Filter
```

PolicyList je-in

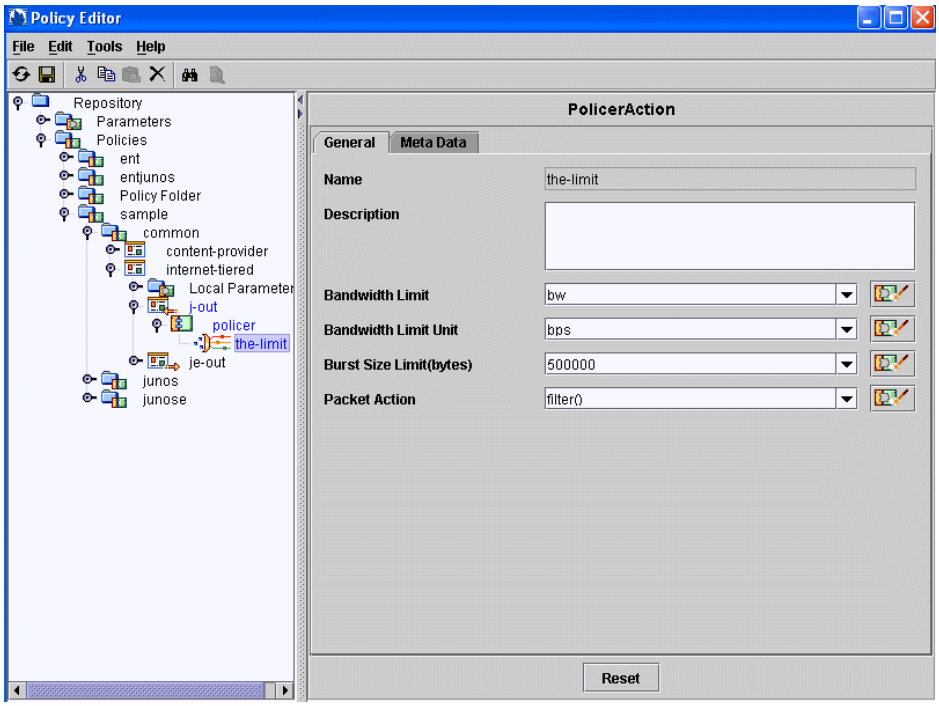
```
        name=je-in
        policyRoles=JUNOSE
        applicability=input

   PolicyRule: name=the-limit
        Priority=600
        type=JUNOSE
        accountingRule=true
     ClassifyTrafficCondition
     RateLimit Action
        rateLimitType=two_rate
        committedRate=bw
        committedBurst=500000
        peakRate=bw
        peakBurst=500000
        committed=Forward
        conformed=Filter
        exceeded=Filter
```

Sample JUNOS Policer Policy

The sample JUNOS policy has a local parameter bw, which is used in the policer action both on input and output directions.

In this example, packets that exceed the bandwidth limit are filtered.

Figure 35: Policer Action for Tiered Internet Service



The following information shows the configuration details of the Internet tiered policy group for JUNOS routing platforms.

policyGroupName=internet-tiered,ou=common,ou=sample,o=Policies,o=umc

Local Parameter

```
name=bw, defaultValue=5000000, parameterType=rate
```

PolicyList j-out

```
        name=j-out
        policyRoles=JUNOS
        applicability=output

PolicyRule: name=the-limit
        priority=600
        type=JUNOS
        accountingRule=true
     Policer Action
        bandwidthLimit=bw
        Burst=500000
        packetAction=filter
```

PolicyList j-in

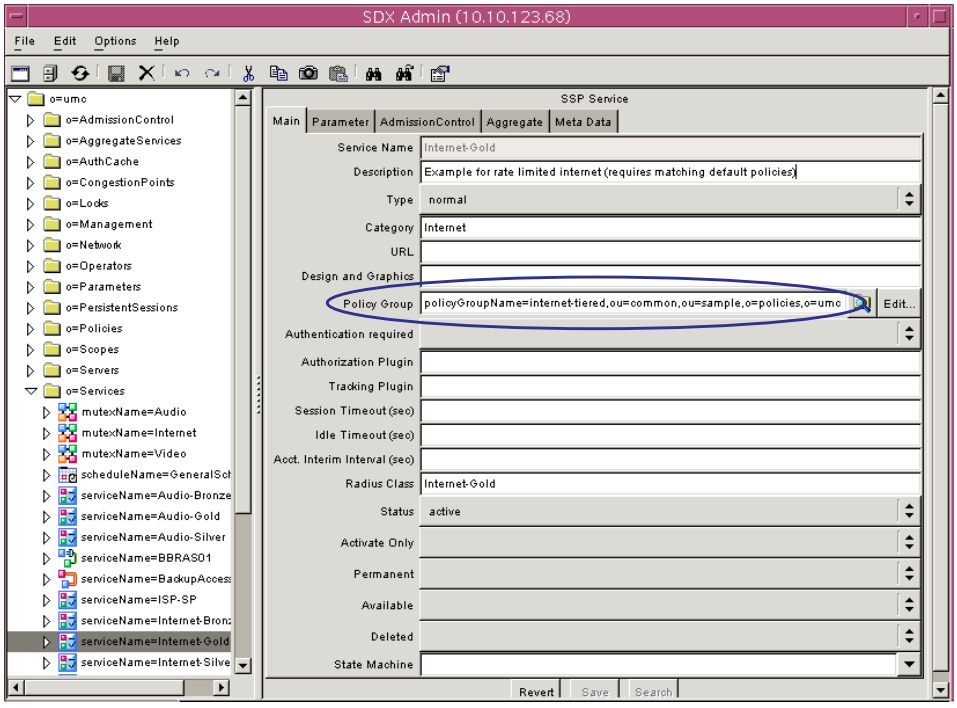
```
        name=j-in
        policyRoles=JUNOS
        applicability=input

     Policer Action
        bandwidthLimit=bw
        burst=500000
        packetAction=filter
```

Defining the Tiered Internet Services

You need to create three value-added (SSP) services—Gold, Silver, and Bronze.

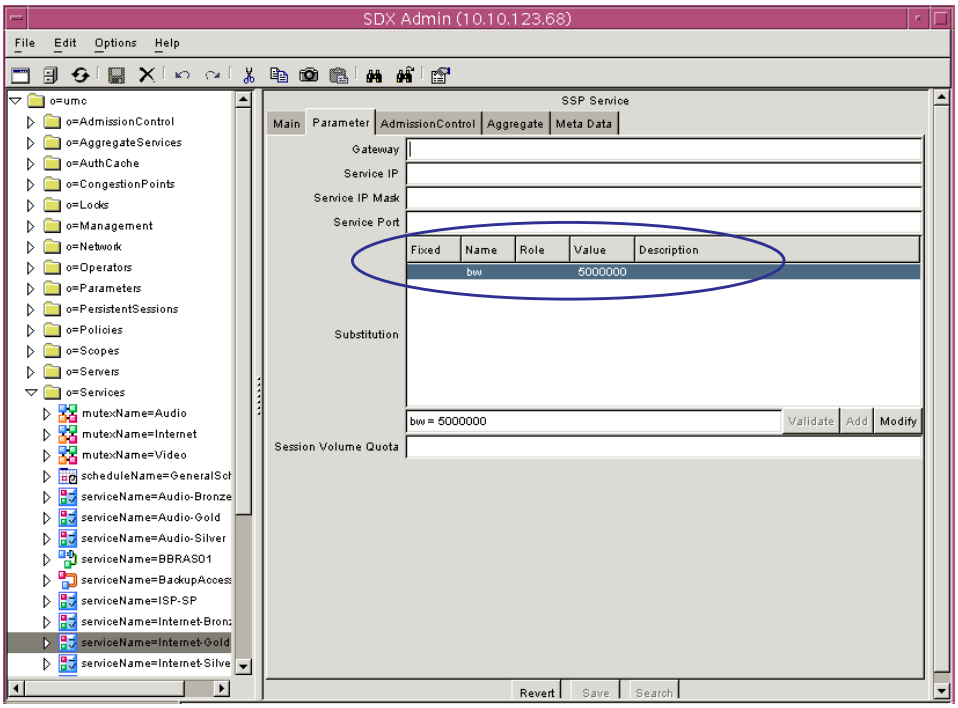
As shown in Figure 36, assign to the new service one of the Internet-tiered policy groups that we created in the last section.

Figure 36: Sample Value-Added Service for Internet Gold Service



For each service, define a substitution value for the bw parameter. For the Gold service, the bw value is 5 Mbps; for the Silver service, the bw value is 1Mbps; and for the Bronze service, the bw value is 64 Kbps. Figure 37 shows how the substitution value is configured for the Gold service.

Figure 37: Parameter Pane of Internet Gold Service



Internet-Gold Service

```
serviceName=Internet-Gold,o=Services,o=umc
policyGroupName:internet-tiered,ou=common,ou=sample,o=Policies,o=umc
substitution:
  bw=5000000
```

Internet-Silver Service

```
serviceName=Internet-Silver,o=Services,o=umc
policyGroupName:internet-tiered,ou=common,ou=sample,o=Policies,o=umc
substitution:
  bw=1000000
```

Internet-Bronze Service

```
serviceName=Internet-Bronze,o=Services,o=umc
policyGroupName:internet-tiered,ou=common,ou=sample,o=Policies,o=umc
substitution:
  bw=64000
```

Example: Providing Premium Services

This scenario shows how service providers can offer premium services, such as video on demand, video conferencing, and voice over IP (VoIP). These types of services are turned on for short periods of time while the premium service is being used.

In this example, two content providers provide premium services. One provides a music service, and the other provides a news service.

Types of Policies

The policy used for premium services depends on the type of service being used. Generally, policies with filter, forward, rate-limit or policer actions, and QoS features are used.

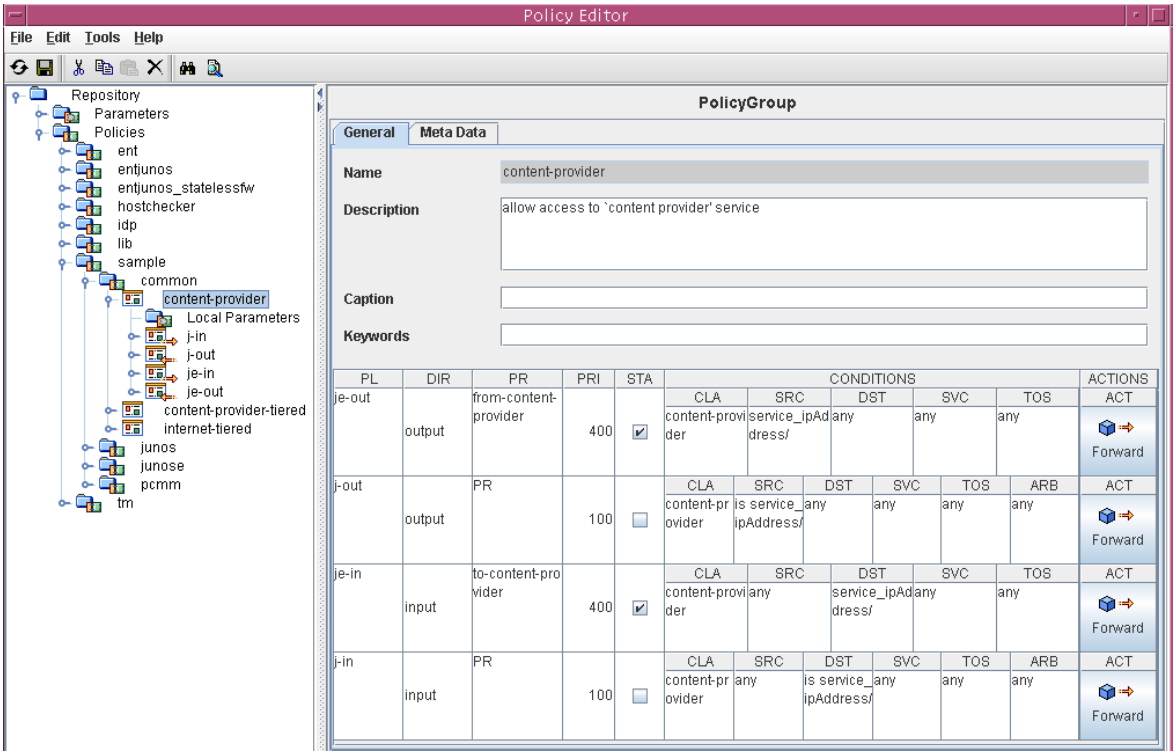
The policy rules in premium services typically have a higher priority (smaller precedence number) than other services and default policies. In this case, the policy rules in the content provider service policies have a priority of 400. The default policy rule has a priority of 500.

The default policy uses the next-hop action to send all traffic destined for the networks of these content providers to the SSP (see *Sample Access Policies* on page 380). When the content provider service is activated, the forward action is taken for packets destined for the content provider network.

Sample JUNOS and JUNOSe Content Provider Policies

The sample content provider policy group includes policy lists for both JUNOS and JUNOSe policies. Figure 38 shows a summary of the content provider policy group.

Figure 38: Premium Service Policy Group



The following information shows the configuration details of the premium service policy group shown in Figure 38.

policyGroupName=content-provider,ou=common,ou=sample,o=Policies,o=umc

PolicyList je-out

```
        name=je-out
        policyRoles=JUNOSE
        applicability=output

   PolicyRule PR
        priority=400
        type=JUNOSE
        accountingRule=true

     ClassifyTrafficCondition
        SourceNetwork:
          ipAddress=service_ipAddress
          ipMask=service_ipMask
          ipOperation=is

     Forward Action
```

PolicyList j-out

```
        name=j-out
        policyRoles=JUNOS
        applicability=output

   PolicyRule PR
        priority=400
        type=JUNOS FILTER
        accountingRule=true

     ClassifyTrafficCondition
        SourceNetwork:
          ipAddress=service_ipAddress
          ipMask=service_ipMask
          ipOperation=is

     Forward Action
```

PolicyList je-in

```
        name=je-in
        policyRoles=JUNOSE
        applicability=input
   PolicyRule: name=PR
        priority=400
        type=JUNOSE
        accountingRule=true

     ClassifyTrafficCondition
        DestinationNetwork:
          ipAddress=service_ipAddress
          ipMask=service_ipMask
          ipOperation=is

     Forward Action
```

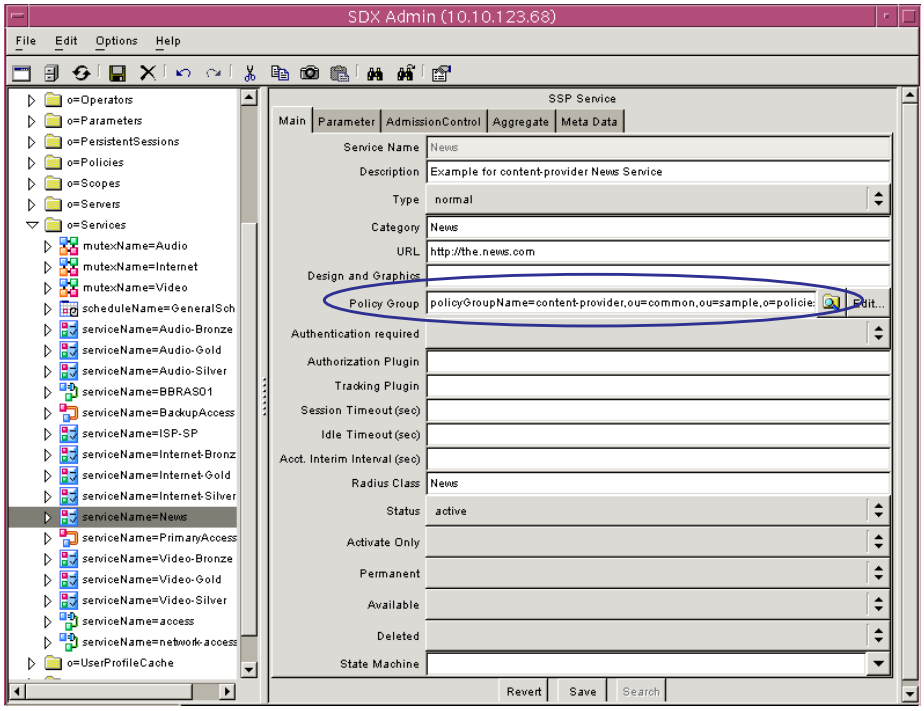
PolicyList j-in

```
        name=j-in
        policyRoles=JUNOS
        applicability=input
   PolicyRule: name=PR
        priority=400
        type=JUNOS FILTER
        accountingRule=true

     ClassifyTrafficCondition
        DestinationNetwork:
          ipAddress=service_ipAddress
          ipMask=service_ipMask
          ipOperation=is

     Forward Action
```

Defining the Premium Services

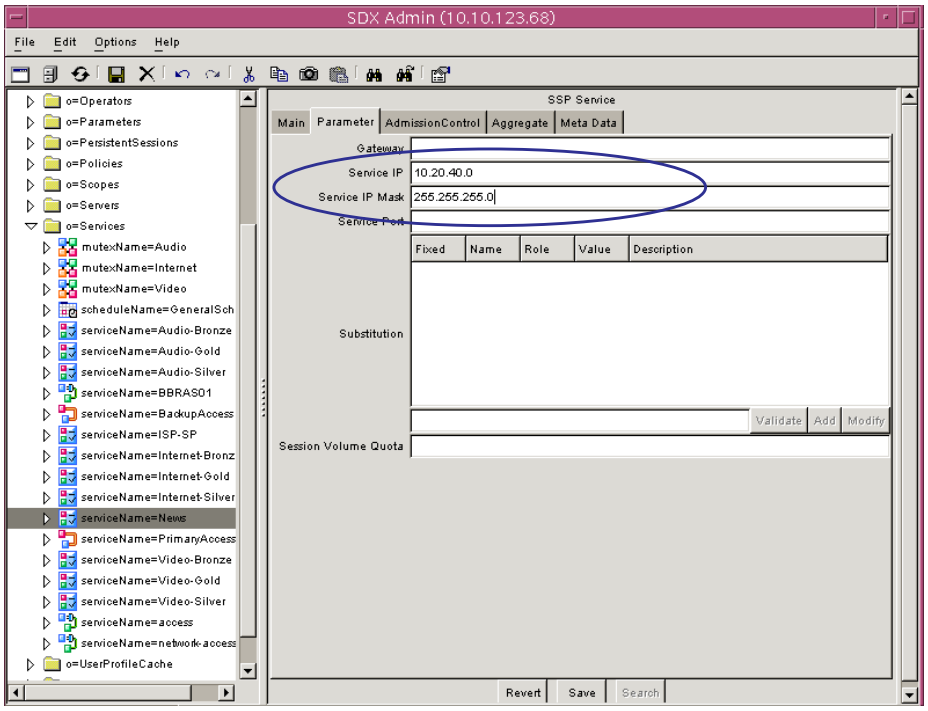
You need to create two value-added (SSP) services—one for the news service and one for the music service. As shown in Figure 39, assign to the new service- the content-provider policy group that we created in the last section.

Figure 39: Sample Value-Added News Service



For each service, define a substitution value for the service_ipAddress and service_ipMask parameters. (See Figure 40.) Note that each content provider has a different service_ipAddress parameter.

Figure 40: Parameter Pane of News Service



Music Service

The music service is provided by the XYZ company, which is a content provider.

```
serviceName=Music,o=Services,o=umc
policyGroupName: content-provider,ou=common,ou=sample,o=Policies,o=umc
substitution:
  service_ipAddress=10.20.30.0
  service_ipMask=255.255.255.0
```

News Service

The news service is provided by the ABC company, which is a content provider.

```
serviceName=News,o=Services,o=umc
policyGroupName: content-provider,ou=common,ou=sample,o=Policies,o=umc
substitution:
  service_ipAddress=10.20.40.0
  service_ipMask=255.255.255.0
```