Chapter 12
Policy Examples Created with the SRC CLI

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 the SRC CLI. To see these examples created with Policy Editor, see *Chapter 13, Policy Examples Created with Policy Editor*.

Topics in this chapter include:

- Example: Creating Access Policies for Subscribers on page 367

- Example: Providing Tiered Internet Services with Policing on page 371

- Example: Providing Premium Services on page 376

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 SAE 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 means of a next-hop action that forwards traffic to the virtual IP address of the portal. (See *SRC-PE Sample Applications Guide*.)

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

DHCP Policy Group

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

Policy List Out

```
[edit policies folder sample folder junose group DHCP list out]
user@host# show
role junose-ipv4;
applicability output;
rule forward {
  type junose-ipv4;
  precedence 500;
  forward forward {
  }
  traffic-condition any {
  }
}
```

Policy List In

```
[edit policies folder sample folder junose group DHCP list in]
user@host# show
role junose-ipv4;
applicability input;
rule forward-to-SSP {
  type junose-ipv4;
  precedence 200;
  forward forward {
  }
  traffic-condition ssp {
    destination-network {
      network {
        ip-address virtual_ipAddress;
        ip-mask 255.255.255.255;
        ip-operation 1;
      }
    }
  }
}
```

```
rule forward-cl-dhcp {
  type junose-ipv4;
  precedence 200;
  forward Fo {
  }
  traffic-condition cl-dhcp {
    protocol-port-condition {
      protocol udp;
      protocol-operation is;
      ip-flags 0;
      ip-flags-mask 0;
      destination-port {
        port {
          port-operation eq;
          from-port 67;
        }
      }
      source-port {
        port {
          port-operation neq;
        }
      }
    }
  }

}
rule cp-to-ssp {
  type junose-ipv4;
  precedence 500;
  next-hop to-ssp {
    next-hop-address virtual_ipAddress;
  }
  traffic-condition content-provider-network-1 {
    destination-network {
      network {
        ip-address 10.10.40.0;
        ip-mask 255.255.255.0;
        ip-operation 1;
      }
    }
  }
  traffic-condition content-provider-network-2 {
    destination-network {
      network {
        ip-address 172.16.0.0;
        ip-mask 255.255.0.0;
        ip-operation 1;
      }
    }
  }
}
```

PPP Policy Group

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

Policy List Out

```
[edit policies folder sample folder junose group PPP list out]
user@host# show
role junose-ipv4;
applicability output;
rule forward {
  type junose-ipv4;
  precedence 500;
  forward forward {
  }
  traffic-condition any {
  }
}
```

Policy List In

```
[edit policies folder sample folder junose group PPP list in]
user@host# show
role junose-ipv4;
applicability input;
rule forward-to-SAE {
  type junose-ipv4;
  precedence 200;
  forward forward {
  }
  traffic-condition sae {
    destination-network {
      network {
        ip-address virtual_ipAddress;
        ip-mask 255.255.255.255;
        ip-operation 1;
      }
    }
  }
}
rule cp-to-ssp {
  type junose-ipv4;
  precedence 500;
  next-hop to-ssp {
    next-hop-address virtual_ipAddress;
  }
  traffic-condition content-provider-network-1 {
    destination-network {
      network {
        ip-address 10.10.40.0;
        ip-mask 255.255.255.0;
        ip-operation 1;
      }
    }
  }
```

```
traffic-condition content-provider-network-2 {
  destination-network {
    network {
      ip-address 172.16.0.0;
      ip-mask 255.255.0.0;
      ip-operation 1;
    }
  }
}
}
```

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 can 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.

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

Local Parameter

```
[edit policies folder sample folder common group internet-tiered
local-parameters]
user@host# show
parameter bw {
  default-value 5000000;
  type rate;
}
```

Policy List je-out

```
[edit policies folder sample folder common group internet-tiered list
je-out]
user@host# show
role junose-ipv4;
applicability output;
rule the-limit {
  type junose-ipv4;
  precedence 600;
  accounting;
  rate-limit limit {
    committed-action {
      forward {
      }
    }
    conformed-action {
      filter {
      }
    }
    exceed-action {
      filter {
      }
    }
    type two_rate;
    committed-rate bw;
    committed-burst 500000;
    peak-rate bw;
    peak-burst 500000;
  }
  traffic-condition any {
  }
}
```

Policy List je-in

```
[edit policies folder sample folder common group internet-tiered list je-in]
user@host# show
role junose-ipv4;
applicability input;
rule the-limit {
  type junose-ipv4;
  precedence 600;
  accounting;
  rate-limit limit {
    committed-action {
      forward {
      }
    }
    conformed-action {
      filter {
      }
    }
    exceed-action {
      filter {
      }
    }
    type two_rate;
    committed-rate bw;
    committed-burst 500000;
    peak-rate bw;
    peak-burst 500000;
  }
  traffic-condition any {
  }
}
```

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.

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

Local Parameter

```
[edit policies folder sample folder common group internet-tiered
local-parameters]
user@host# show
parameter bw {
  default-value 5000000;
  type rate;
}
```

PolicyList j-out

```
[edit policies folder sample folder common group internet-tiered list j-out]
user@host# show
role junos;
applicability output;
rule PR {
  type junos-filter;
  precedence 100;
  policer PA {
    packet-action packet0 {
      filter {
      }
    }
    bandwidth-limit bw;
    bandwidth-limit-unit bps;
    burst 15000;
  }
}
```

PolicyList j-in

```
[edit policies folder sample folder common group internet-tiered list j-in]
user@host# show
role junos;
applicability input;
rule PR {
  type junos-filter;
  precedence 100;
  policer PA {
    packet-action packet0 {
      filter {
      }
    }
    bandwidth-limit bw;
    bandwidth-limit-unit bps;
    burst 15000;
  }
}
```

Defining the Tiered Internet Services

You need to create three SAE services—Gold, Silver, and Bronze.

Assign to the new service one of the Internet-tiered policy groups that we created in the last section.

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.

Internet-Gold Service

```
[edit services global service Internet-Gold]
user@host# show
description "Example for rate limited internet (requires matching default
policies)";
type normal;
category Internet;
policy-group /sample/common/internet-tiered;
radius-class Internet-Gold;
status active;
parameter {
  substitution "bw = 5000000";
}
```

Internet-Silver Service

```
[edit services global service Internet-Silver]
user@host# show
description "Example for rate limited internet (requires matching default
policies)";
type normal;
category Internet;
policy-group /sample/common/internet-tiered;
radius-class Internet-Silver;
status active;
parameter {
  substitution "bw = 1000000";
}
```

Internet-Bronze Service

```
[edit services global service Internet-Bronze]
user@host# show
description "Example for rate limited internet (requires matching default
policies)";
type normal;
category Internet;
policy-group /sample/common/internet-tiered;
radius-class Internet-Bronze;
status active;
parameter {
  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 portal (see *Sample Access Policies* on page 368). 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. The following information shows the configuration details of the premium service policy group.

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

PolicyList je-out

```
[edit policies folder sample folder common group content-provider list
je-out]
user@host# show
role junose-ipv4;
applicability output;
rule from-content-provider {
  type junose-ipv4;
  precedence 400;
  accounting;
  forward forward {
  }
  traffic-condition content-provider {
    source-network {
      network {
        ip-address service_ipAddress;
        ip-mask service_ipMask;
        ip-operation 1;
      }
    }
  }
}
```

PolicyList j-out

```
[edit policies folder sample folder common group content-provider list
j-out]
user@host# show
role junos;
applicability output;
rule PR {
  type junos-filter;
  precedence 100;
  forward FA {
  }
  traffic-condition content-provider {
    source-network {
      network {
        ip-address service_ipAddress;
        ip-mask service_ipMask;
        ip-operation is;
      }
    }
  }
}
```

PolicyList je-in

```
[edit policies folder sample folder common group content-provider list
je-in]
user@host# show
role junose-ipv4;
applicability input;
rule to-content-provider {
  type junose-ipv4;
  precedence 400;
  accounting;
  forward forward {
  }
  traffic-condition content-provider {
    destination-network {
      network {
        ip-address service_ipAddress;
        ip-mask service_ipMask;
        ip-operation 1;
      }
    }
  }
}
```

PolicyList j-in

```
[edit policies folder sample folder common group content-provider list j-in]
user@host# show
role junos;
applicability input;
rule PR {
  type junos-filter;
  precedence 100;
  forward FA {
  }
```

```
        traffic-condition content-provider {
          destination-network {
            network {
              ip-address service_ipAddress;
              ip-mask service_ipMask;
              ip-operation is;
            }
          }
        }
      }
```

Defining the Premium Services

You need to create two SAE services—one for the news service and one for the music service. Assign to the new service the content-provider policy group that we created in the last section.

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

Music Service

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

```
[edit services global sae-service Music]
user@host# show
type normal;
policy-group /sample/content-provider;
status active;
available;
parameter {
  service-ip-address 10.20.30.0;
  service-ip-mask 255.255.255.0;
}
```

News Service

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

```
[edit services global sae-service News]
user@host# show
description "Example for content-provider in different network";
type normal;
category News;
url http://the.news.com;
policy-group /sample/common/content-provider;
radius-class News;
status active;
parameter {
  service-ip-address 10.20.40.0;
  service-ip-mask 255.255.255.0;
}
```