

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.

From the service provider's perspective, the service provider's network is on the inside, and the enterprise network is on the outside. Ingress traffic flows from the enterprise network to the service provider's network. Egress traffic flows from the service provider's network to the enterprise network.

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;
            }
        }
    }
}
}

```