Option: Using IPSec with a Layer 3 VPN

Some key concepts to keep in mind when configuring IPSec within a VPN include the following:

- Add the outside services interface for a next-hop style service set into the routing instance by including the interface sp-*fpc/pic/port* statement at the [edit routing-instances *instance-name*] hierarchy level.
- For interface style service sets, add the interface on which you apply the service set and the services interface by including both interfaces at the [edit routing-instances *instance-name*] hierarchy level.
- To define a routing instance for the local gateway within the service set, include the routing-instance *instance-name* option at the [edit services service-set *service-set-name* ipsec-vpn-options local-gateway *address*] hierarchy level.

The following configuration for an AS PIC on a provider edge (PE) router demonstrates the use of next-hop service sets with an IKE dynamic SA in a VPN routing and forwarding (VRF) routing instance.

```
[edit]
interfaces {
    so-0/0/0 {
        description "Interface connected to the customer edge (CE) router";
        unit 0 {
            family inet {
                address 10.6.6.6/32;
            }
        }
    }
    so-2/2/0 {
        description "Source IPSec tunnel interface to the network core";
        unit 0 {
            family inet {
                address 10.10.1.1/30;
            }
        }
    }
    sp-3/1/0 {
        description "AS PIC interface";
        unit 0 {
            family inet {
                address 10.7.7.7/32;
            }
        }
        unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
```

```
    }
}
policy-options {
    policy-statement vpn-export-policy {
        then {
            community add community-name;
            accept;
        }
    }
    policy-statement vpn-import-policy {
        term term-name {
            from community community-name;
            then accept;
        }
    }
    community community-name members target:100:20;
}
routing-instances {
    vrf {
        instance-type vrf;
        interface sp-3/1/0.1; # Inside sp interface.
        interface so-0/0/0.0; # Interface that connects to the CE router.
        route-distinguisher route-distinguisher;
        vrf-import vpn-import-policy;
        vrf-export vpn-export-policy;
        routing-options {
            static {
                route ip-address/prefix next-hop so-0/0/0.0; # Routes for the CE router.
                route ip-address/prefix next-hop sp-3/1/0.1; # Routes for IPSec.
            }
        }
    }
}
services {
    service-set service-set-name {
        next-hop-service {
            inside-service-interface sp-3/1/0.1;
            outside-service-interface sp-3/1/0.2;
        }
        ipsec-vpn-options {
            local-gateway 10.10.1.1;
        }
        ipsec-vpn-rules rule-name;
    }
    ipsec-vpn {
        rule rule-name {
            term term-name {
                from {
                    source-address {
                        source-ip-address;
                    }
                }
                then {
                    remote-gateway 10.10.1.2;
                    dynamic {
                        ike-policy ike-policy-name;
```

```
                }
              }
            }
            match-direction direction;
          }
          ike {
            policy  ike-policy-name  {
              pre-shared-key ascii-text preshared-key;
            }
          }
        }
      }
```

For more information on VRF routing instances, see the *JUNOS VPNs Configuration Guide*. For more information on next-hop service sets, see the *JUNOS Services Interfaces Configuration Guide*.

Published: 2010-04-15