

Chapter 21

Configuring Encryption Interfaces

The Internet Protocol Security (IPSec) architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and non-repudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

IPSec defines a security association (SA) and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. For more information, see the *JUNOS System Basics Configuration Guide*. The standards are defined in the following RFCs:

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

To enable encryption interfaces, you can configure the following properties:

Configuring an Encryption Interface on page 338

Configuring ES PIC Redundancy on page 339

Configuring IPSec Tunnel Redundancy on page 341

For detailed information about configuring the ES PIC, see the *JUNOS Services Interfaces Configuration Guide*.

Configuring an Encryption Interface

When you configure the encryption interface, you associate the configured SA with a logical interface. This configuration defines the tunnel, including the logical unit, tunnel addresses, maximum transmission unit (MTU), optional interface addresses, and the name of the IPsec SA to apply to traffic. To configure an encryption interface, include the following statements:

```
family inet {
  ipsec-sa ipsec-sa;           # name of security association to apply to packet
  address address {           # local interface address inside local VPN
    destination address;      # destination address inside remote VPN
  }
}
tunnel {
  source source-address;
  destination address;
}
```

You can include these statements at the following hierarchy levels:

```
[edit interfaces interface-name unit logical-unit-number]
```

```
[edit logical-routers logical-router-name interfaces interface-name unit
logical-unit-number]
```

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.



NOTE: You must configure the tunnel source address locally on the routing platform, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs.

Specifying the Security Association Name

The security association is the set of properties that defines the protocols for encrypting internet traffic. To configure encryption interfaces, you specify the SA name associated with the interface by including the `ipsec-sa sa-name` statement at the `[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]` hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
ipsec-sa sa-name;
```

For information about configuring the security association, see “Configuring ES PIC Redundancy” on page 339.

Example: Configuring an Encryption Interface

Configure an IPsec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The `ipsec-sa` statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5;           # tunnel source address
      destination 10.6.6.6;     # tunnel destination address
    }
    family inet {
      ipsec-sa manual-sa1;      # name of security association to apply to packet
      mtu 3800;
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

Configuring ES PIC Redundancy

You can configure ES PIC redundancy for routing platforms that can have multiple ES PICs. With ES PIC redundancy, one ES PIC is active and another ES PIC is on standby. When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and SAs, and acts as the new next hop for IPsec traffic. Reestablishment of tunnels on the backup ES PIC does not require new IKE negotiations. If the primary ES PIC comes online, it remains in standby and does not preempt the backup. To determine which PIC is currently active, use the `show ipsec redundancy` command.



NOTE: ES PIC redundancy is supported on M-series routing platforms only.

To configure an ES PIC as the backup, include the `backup-interface` statement at the `[edit interfaces es-fpc/pic/port es-options]` hierarchy level:

```
[edit interfaces es-fpc/pic/port es-options]
backup-interface es-fpc/pic/port;
```

Example: Configuring ES PIC Redundancy

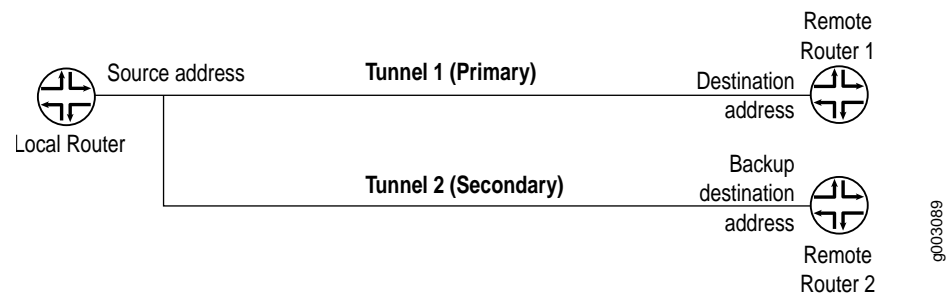
After you create the inbound firewall filter, apply it to the master ES PIC. Here, the inbound firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. The IPsec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and decrypts the incoming packet. This example does not show SA and filter configuration. For information about SA and filter configuration, see the *JUNOS System Basics Configuration Guide*, the *JUNOS Policy Framework Configuration Guide*, and the *JUNOS Services Interfaces Configuration Guide*.

```
[edit interfaces]
  es-1/2/0 {
    es-options {
      backup-interface es-1/0/0;
    }
    unit 0 {
      tunnel {
        source 10.5.5.5;
        destination 10.6.6.6;
      }
      family inet {
        ipsec-sa manual-sa1;
        filter {
          input ipsec-decrypt-policy-filter;
        }
        address 10.1.1.8/32 {
          destination 10.2.2.254;
        }
      }
    }
  }
}
```

Configuring IPsec Tunnel Redundancy

You can configure IPsec tunnel redundancy by specifying a backup destination address. The local routing platform sends keepalives to determine the remote site's reachability. When the peer is no longer reachable, a new tunnel is established. For up to 60 seconds during failover, traffic is dropped without notification being sent. Figure 26 shows IPsec primary and backup tunnels.

Figure 26: IPsec Tunnel Redundancy



To configure IPsec tunnel redundancy, include the `backup-destination` statement at the [edit interfaces unit *logical-unit-number* tunnel] hierarchy level:

```
[edit interfaces unit logical-unit-number]
  tunnel {
    backup-destination address;
    destination address;
    source address;
  }
```



NOTE: Tunnel redundancy is supported on M-series routing platforms only.

The primary and backup destinations must be on different routing platforms.

The tunnels should be diverse and policies should match.

For more information about tunnels, see “Configuring Tunnel Interfaces” on page 569.

