

Chapter 24

Encryption Interfaces Configuration Guidelines

The Internet Protocol Security (IPSec) architecture provides a security suite for the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (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 288

Configuring Traffic on page 289

Configuring an ES Tunnel Interface for a Layer 3 VPN on page 295

Configuring ES PIC Redundancy on page 296

Configuring IPSec Tunnel Redundancy on page 297

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 at the [edit interfaces *es-fpc/pic/port* unit *logical-unit-number*] hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number]
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-address source-address;
  destination destination-address;
}
```

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 router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The ES Physical Interface Card (PIC) is supported on M-series and T-series routing platforms.

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 Traffic” on page 289.

Configuring the MTU for an Encryption Interface

The protocol MTU value for encryption interfaces must always be less than the default interface MTU value of 3900 bytes; the configuration fails to commit if you select a greater value. To set the MTU value, include the `mtu bytes` statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
mtu bytes;
```

For more information, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

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 Traffic

This section contains the following topics:

Traffic Overview on page 290

Configuring the Security Association on page 291

Configuring an Outbound Traffic Filter on page 292

Applying the Outbound Traffic Filter on page 293

Configuring an Inbound Traffic Filter on page 293

Applying the Inbound Traffic Filter to the Encryption Interface on page 294

Traffic Overview

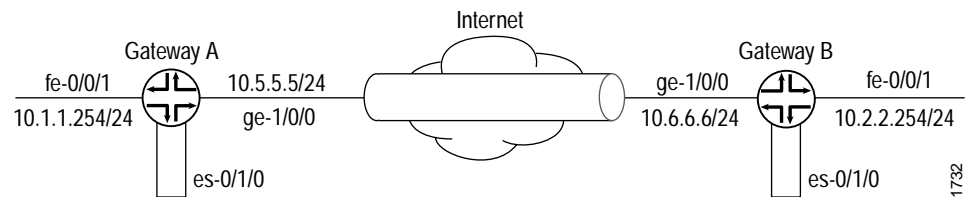
Traffic configuration defines the traffic that must flow through the tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure that the configuration is correct.



NOTE: The valid firewall filters statements for IPSec are destination-port, source-port, protocol, destination-address, and source-address.

In Figure 1, Gateway A protects the network 10.1.1.0/24, and Gateway B protects the network 10.2.2.0/24. The gateways are connected by an IPSec tunnel. For more information about firewalls, see the *JUNOS Policy Framework Configuration Guide*.

Figure 1: Example: IPSec Tunnel Connecting Security Gateways



The SA and ES interface for security Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text 123456789009876543211234;
      }
    }
  }
}
```

```
[edit interfaces es-0/1/0]
  unit 0 {
    tunnel {
      source 10.5.5.5;
      destination 10.6.6.6;
    }
    family inet {
      ipsec-sa manual-sa1;
      address 10.1.1.8/32 {
        destination 10.2.2.254;
      }
    }
  }
}
```

Configuring the Security Association

To configure the SA, include the following statements at the [edit security] hierarchy level:

```
[edit security]
  security-association name {
    mode (tunnel | transport);
    manual {
      direction (inbound | outbound | bi-directional) {
        auxiliary-spi auxiliary-spi-value;
      }
      spi spi-value;
      protocol (ah | esp | bundle);
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
    }
    dynamic {
      replay-window-size (32 | 64);
      ipsec-policy policy-name;
    }
  }
}
```

For more information about configuring an SA, see the *JUNOS Systems Basics Configuration Guide*. For information about applying the SA to an interface, see “Specifying the Security Association Name” on page 288.

Configuring an Outbound Traffic Filter

To configure the outbound traffic filter, include the following statements at the [edit firewall] hierarchy level:

```
filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}
```

For more information, see the *JUNOS Policy Framework Configuration Guide*.

Example: Configuring an Outbound Traffic Filter

Firewall filters for outbound traffic direct the traffic through the desired IPsec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see Figure 1 on page 290). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal virtual private network (VPN) traffic:

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address {      # local network
        10.1.1.0/24;
      }
      destination-address { # remote network
        10.2.2.0/24;
      }
    }
    then ipsec-sa manual-sa1; # apply SA name to packet
  }
  term default {
    then accept;
  }
}
```



NOTE: The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

Applying the Outbound Traffic Filter

After you have configured the outbound firewall filter, you apply it by including the following statements at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]
filter {
    input filter-name;
}
```

Example: Applying the Outbound Traffic Filter

Apply the outbound traffic filter. The outbound filter is applied on the Fast Ethernet interface at the [edit interfaces fe-0/0/1 unit 0 family inet] hierarchy level. Any packet matching the IPsec action term (term 1) on the input filter (ipsec-encrypt-policy-filter), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the [edit interfaces es-0/1/0 unit 0 family inet] hierarchy level. So, if a packet arrives from the source address 10.1.1.0/24 and goes to the destination address 10.2.2.0/24, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the manual-sa1 SA. The ES PIC receives the packet, applies the manual-sa1 SA, and sends the packet through the tunnel.

The router must have a route to the tunnel end point; add a static route if necessary.

```
[edit interfaces]
fe-0/0/1 {
    unit 0 {
        family inet {
            filter {
                input ipsec-encrypt-policy-filter;
            }
            address 10.1.1.254/24;
        }
    }
}
```

Configuring an Inbound Traffic Filter

To configure an inbound traffic filter, include the following statements at the [edit firewall] hierarchy level:

```
filter filter-name {
    term term-name {
        from {
            match-conditions;
        }
        then {
            action;
            action-modifiers;
        }
    }
}
```

For more information, see the *JUNOS Policy Framework Configuration Guide*.

Example: Configuring an Inbound Traffic Filter

Configure an inbound firewall filter. This filter performs the final IPSec policy check and is created on security gateway A. The policy check ensures that only packets that match the traffic configured for this tunnel are accepted.

```
[edit firewall]
filter ipsec-decrypt-policy-filter {
  term term1 {                               # perform policy check
    from {
      source-address {                       # remote network
        10.2.2.0/24;
      }
      destination-address {                 # local network
        10.1.1.0/24;
      }
    }
  }
  then accept;
}
}
```

Applying the Inbound Traffic Filter to the Encryption Interface

After you create the inbound firewall filter, you can apply it to the ES PIC. To apply the filter to the ES PIC, include the filter statement at the [edit interfaces *es-fpc/pic/port* unit *logical-unit-number* family inet filter] hierarchy level:

```
[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]
filter {
  input filter;
}
}
```

The input filter is the name of the filter applied to received traffic. For a configuration example, see “Example: Configuring an Inbound Traffic Filter” on page 294. For more information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

Example: Applying the Inbound Traffic Filter to the Encryption Interface

Apply the inbound firewall filter (ipsec-decrypt-policy-filter) to 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.

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's security parameter index (SPI), protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPsec manual-sa1 SA is referenced at the [edit interfaces es-1/2/0 unit 0 family inet] hierarchy level and is used to decrypt the incoming packet. When the packets are processed (decrypted, authenticated, or both), the input firewall filter (ipsec-decrypt-policy-filter) is applied on the decrypted packet to perform the final policy check. term1 defines the decrypted (and verified) traffic and performs the required policy check. For information about term1, see “Example: Configuring an Inbound Traffic Filter” on page 294.



NOTE: The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

```
[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5;           # tunnel source address
      destination 10.6.6.6;     # tunnel destination address
    }
    family inet {
      filter {
        input ipsec-decrypt-policy-filter;
      }
      ipsec-sa manual-sa1;      # SA name applied to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

Configuring an ES Tunnel Interface for a Layer 3 VPN

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the provider edge (PE) router and on the customer edge (CE) router. You also need to configure IPsec on the PE and CE routers. For more information about configuring an ES tunnel for a Layer 3 VPN, see the *JUNOS VPNs Configuration Guide*.

Configuring ES PIC Redundancy

You can configure ES PIC redundancy on M-series and T-series routing platforms that 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 and T-series routing platforms.

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

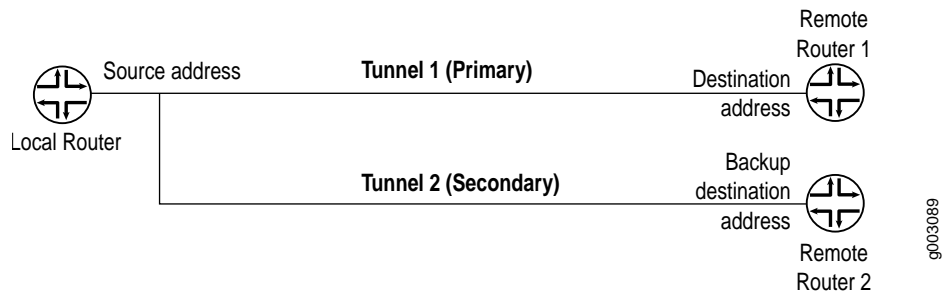
After you create the inbound firewall filter, apply it to the master ES PIC. Here, the inbound firewall filter (`ipsec-decrypt-policy-filter`) is applied on the decrypted packet to perform the final policy check. The IPSec manual-sa1 SA is referenced at the `[edit interfaces es-1/2/0 unit 0 family inet]` 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 “Example: Configuring an Inbound Traffic Filter” on page 294.

```
[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 router 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 2 shows IPsec primary and backup tunnels.

Figure 2: 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 address;
}
```



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

The primary and backup destinations must be on different routers.

The tunnels must be diverse and policies must match.

For more information about tunnels, see “Tunnel Interfaces Configuration Guidelines” on page 491.

