To use IPsec security services, you create an SA between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. You can configure two types of SAs:

- Manual—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see “Configuring Manual IPsec Security Associations for an ES PIC” on page 3.

- Dynamic—Specify proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposal statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see Associating the Configured Security Association with a Logical Interface.

**NOTE:** The JUNOS Software does not perform a commit check when an SA name referenced in the Border Gateway Protocol (BGP) protocol section is not configured at the [edit security ipsec] hierarchy level.

We recommend that you configure no more than 512 dynamic security associations per ES Physical Interface Card (PIC).

To configure an SA for IPsec for an ES PIC, include the security-association statement at the [edit security ipsec] hierarchy level:

```junos
[edit security ipsec]
security-association sa-name;
```

**NOTE:** You configure a dynamic SA for the AS and MultiServices PICs at the [edit services ipsec-vpn rule rule-name term term-name then dynamic], [edit services ipsec-vpn ike], and [edit services ipsec-vpn ipsec] hierarchy levels.

For more information, see the “IPsec” chapter of the *JUNOS Feature Guide* and the “IPsec Services Configuration Guidelines” chapter of the *JUNOS Services Interfaces Configuration Guide*.

Tasks to configure SAs for IPsec for an ES PIC are:
1. Configuring the Description for an SA on page 2
2. Configuring IPsec Transport Mode on page 2
3. Configuring IPsec Tunnel Mode on page 2
Configuring the Description for an SA

To specify a description for an IPsec SA, include the description statement at the edit security ipsec security-association sa-name hierarchy level:

```
[edit security ipsec security-association sa-name]
  description description;
```

Configuring IPsec Transport Mode

In transport mode, the data portion of the IP packet is encrypted, but the IP header is not. Transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. Virtual private network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. You configure manual SAs, and you must configure static values on both ends of the SA.

**NOTE:** When you use transport mode, the JUNOS Software supports both BGP and OSPFv3 for manual SAs.

To configure IPsec security for transport mode, include the mode statement with the transport option at the edit security ipsec security-association sa-name hierarchy level:

```
[edit security ipsec security-association sa-name]
  mode transport;
```

To apply tunnel mode, you configure manual SAs in transport mode and then reference the SA by name at the [edit protocols bgp] hierarchy level to protect a session with a given peer.

**NOTE:** You can configure BGP to establish a peer relationship over encrypted tunnels.

Configuring IPsec Tunnel Mode

You use tunnel mode when you use preshared keys with IKE to authenticate peers, or digital certificates with IKE to authenticate peers. In tunnel mode, encryption services are performed on an ES PIC.

When you use preshared keys, you manually configure a preshared key, which must match that of its peer. With digital certificates, each router is dynamically or manually enrolled with a certificate authority (CA). When a tunnel is established, the public keys used for IPsec are dynamically obtained through IKE and validated against the CA certificate. This avoids the manual configuration of keys on routers within the topology. Adding a new router to the topology does not require any security configuration changes to existing routers.
To configure the IPsec in tunnel mode, include the `mode` statement with the `tunnel` option at the `edit security ipsec security-association sa-name` hierarchy level:

```
[edit security ipsec security-association sa-name]
mode tunnel;
```

**NOTE:** Tunnel mode requires the ES PIC.

The JUNOS Software supports both BGP and OSPFv3 in transport mode.

To enable tunnel mode, follow the steps in these sections:
- Configuring Security Associations for IPsec on an ES PIC on page 1
- Configuring an IKE Proposal for Dynamic SAs
- Associating the Configured Security Association with a Logical Interface
- IPsec Tunnel Traffic Configuration Overview

### Configuring Manual IPsec Security Associations for an ES PIC

To use IPsec security services, you create security associations (SAs) between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. There are two types of SAs: manual and dynamic.

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, peers can communicate only when they all share the same configured options.

To configure the manual IPsec SA for an ES PIC, include the `manual` statement at the `edit security ipsec security-association sa-name` hierarchy level:

```
[edit security ipsec security-association sa-name]
manual {
    direction (inbound | outbound | bi-directional) {
        authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
        }
        auxiliary-spi auxiliary-spi-value;
        encryption {
            algorithm (des-cbc | 3des-cbc);
            key (ascii-text key | hexadecimal key);
        }
        protocol (ah | esp | bundle);
        spi spi-value;
    }
}
```
Tasks to configure a manual SA are:
1. Configuring the Processing Direction on page 4
2. Configuring the Protocol for a Manual SA on page 5
3. Configuring the Security Parameter Index on page 5
4. Configuring the Auxiliary Security Parameter Index on page 6
5. Configuring the Authentication Algorithm and Key on page 6
6. Configuring the Encryption Algorithm and Key on page 7

**Configuring the Processing Direction**

The `direction` statement sets inbound and outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the `inbound` and `outbound` options. If you want the same attributes in both directions, use the `bidirectional` option.

To configure the direction of IPsec processing, include the `direction` statement and specify the direction at the `[edit security ipsec security-association sa-name manual]` hierarchy level:

```
[edit security ipsec security-association sa-name manual]
direction (inbound | outbound | bidirectional);
```

The following example shows how to define different algorithms, keys, and security parameter index values for inbound and outbound processing directions:

```
[edit security ipsec security-association sa-name manual]
manual {
    direction inbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 23456789012345678901234;
        }
        protocol esp;
        spi 16384;
    }
    direction outbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 12345678901234567890abcd;
        }
        protocol esp;
        spi 24576;
    }
}
```

The following example shows how to define the same algorithms, keys, and security parameter index values for bidirectional processing:

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
    encryption {
        algorithm 3des-cbc;
        key ascii-text 23456789012345678901234;
    }
    protocol esp;
    spi 16384;
}
```
IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). For transport mode SAs, both ESP and AH are supported. The AH protocol is used for strong authentication. The bundle option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

**NOTE:** The AH protocol is supported only on M Series routers.

To configure the IPsec protocol on an ES PIC, include the `protocol` statement at the `edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)` hierarchy level and specify the `ah`, `bundle`, or `esp` option:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]
protocol (ah | bundle | esp);
```

**Configuring the Security Parameter Index**

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.

**NOTE:** Each manual SA must have a unique SPI and protocol combination.

Use the auxiliary SPI when you configure the `protocol` statement to use the `bundle` option.

To configure the SPI on an ES PIC, include the `spi` statement and specify a value (256 through 16,639) at the `[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]` hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]
spi spi-value;
```
Configuring the Auxiliary Security Parameter Index

When you configure the protocol statement to use the bundle option, the JUNOS Software uses the auxiliary SPI for the ESP and the SPI for the AH.

**NOTE:** Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the auxiliary-spi statement at the [edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)] hierarchy level and set the value to an integer between 256 and 16,639:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound | bidirectional)]
auxiliary-spi auxiliary-spi-value;
```

**Configuring the Authentication Algorithm and Key**

To configure an authentication algorithm and key, include the authentication statement at the [edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)] hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound | bidirectional)]
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text key**—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal key**—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.
Configuring the Encryption Algorithm and Key

To configure IPsec encryption, include the encryption statement and specify an algorithm and key at the [edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)] hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]
encryption {
    algorithm (des-cbc | 3des-cbc);
    key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.

**NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409. For 3des-cbc, we recommend that the first 8 bytes not be the same as the second 8 bytes, and that the second 8 bytes be the same as the third 8 bytes.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the des-cbc option, the key contains 8 ASCII characters. With the 3des-cbc option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the des-cbc option, the key contains 16 hexadecimal characters. With the 3des-cbc option, the key contains 48 hexadecimal characters.

**NOTE:** You cannot configure encryption when you use the AH protocol.

Configuring Dynamic IPsec Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To configure a dynamic SA, include the `dynamic` statement at the [edit security ipsec security-association sa-name] hierarchy level. Specify an IPsec policy name, and optionally, a 32-packet or 64-packet replay window size.
Enabling Dynamic IPsec Security Associations

To enable a dynamic SA, follow these steps:
1. Configure IKE proposals and IKE policies associated with these proposals.
2. Configure IPsec proposals and an IPsec policy associated with these proposals.
3. Associate an SA with an IPsec policy.

**NOTE:** Dynamic tunnel SAs require an ES PIC. If you want to establish a dynamic SA, the attributes in at least one configured IPsec and IKE proposal must match those of its peer.

The replay window is not used with manual SAs.

Published: 2010-04-26

```plaintext
[edit security ipsec security-association sa-name]
  dynamic {
    ipsec-policy policy-name;
    replay-window-size (32 | 64);
  }
```