

Chapter 29

Summary of Security Services Configuration Statements

The following sections explain each of the security services configuration statements. The statements are organized alphabetically.

authentication

Syntax	<pre>authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); }</pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bi-directional)]
Description	Configure IPSec authentication parameters for manual SA.
Options	<p>algorithm—Hash algorithm that authenticates packet data.</p> <p>The algorithm can be one of the following:</p> <ul style="list-style-type: none">hmac-md5-96—Produces a 128-bit digest,hmac-sha1-96—Produces a 160-bit digest. <p>key—Type of authentication key.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none">ascii-text <i>key</i>—ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters.hexadecimal <i>key</i>—Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.
Usage Guidelines	See “Configure Authentication” on page 318.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm

authentication-algorithm (IKE)

- Syntax** authentication-algorithm (md5 | sha1);
- Hierarchy Level** [edit security ike],
[edit security ike proposal *ike-proposal-name*]
- Description** Configure IKE authentication algorithm.
- Options** authentication-algorithm—Hash algorithm that authenticates packet data.

md5—Produces a 128-bit digest.

sha1—Produces a 160-bit digest.
- Usage Guidelines** See “Configure an IKE Authentication Algorithm” on page 322.
- Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

authentication-algorithm (IPSec)

- Syntax** authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
- Hierarchy Level** [edit security ipsec],
[edit security ipsec proposal *ipsec-proposal-name*]
- Description** Configure IPSec authentication algorithm.
- Options** authentication-algorithm—Hash algorithm that authenticates packet data.

hmac-md5-96—Produces a 128-bit digest.

hmac-sha1-96—Produces a 160-bit digest.
- Usage Guidelines** See “Configure an Authentication Algorithm” on page 327.
- Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

authentication-method

Syntax	authentication-method pre-shared-keys;
Hierarchy Level	[edit security ike], [edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure IKE authentication method.
Options	pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange.
Usage Guidelines	See “Configure an IKE Authentication Method” on page 322.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

dh-group

Syntax	dh-group (group1 group2);
Hierarchy Level	[edit security ike], [edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the IKE Diffie-Hellman group.
Options	dh-group—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
	The dh group can be one of the following:
	group1—768 bit.
	group2—1,024-bit.
Usage Guidelines	See “Configure an IKE Diffie-Hellman Group” on page 323.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.


direction

- Syntax** direction (inbound | outbound | bidirectional);
- Hierarchy Level** [edit security ipsec security-association *name* manual]
- Description** Define the direction of the SA.
- Options**
 - direction—Direction of IPSec processing.
 - inbound—Inbound SA.
 - outbound—Outbound SA.
 - bidirectional—Bidirectional SA.
- Usage Guidelines** See “Configure Direction” on page 316.
- Required Privilege Level**
 - system—To view this statement in the configuration.
 - system-control—To add this statement to the configuration.

dynamic

- Syntax** dynamic ipsec-policy *ipsec-policy-name*;
- Hierarchy Level** [edit security ipsec security-association *name*]
- Description** Define a dynamic IPSec SA.
- Usage Guidelines** See “Configure the ES PIC” on page 330.
- Required Privilege Level**
 - admin—To view this statement in the configuration.
 - admin-control—To add this statement to the configuration.

encryption

Syntax	<pre> encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } </pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bidirectional)]
Description	Configure an encryption algorithm and key for manual SA.
Options	<p>algorithm—Type of encryption algorithm.</p> <p>The algorithm can be one of the following:</p> <ul style="list-style-type: none"> des-cbc—Has a block size of 8 bytes (64 bits); its key size is 48 bits long. 3des-cbc—Has block size of 8 bytes (64 bits); its key size is 192 bits long. <div style="border: 1px solid black; padding: 10px; margin: 10px 0;">  <p>Note For 3des-cbc, the first 8 bytes must not be same as the second 8 bytes, and the second 8 bytes must not be same as the third 8 bytes.</p> </div> <p>key—Type of encryption key.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none"> ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters. hexadecimal—Hexadecimal key. For the des-cbc option, the key contains 16 hexadecimal characters; for the 3des-cbc option, the key contains 48 hexadecimal characters.
Usage Guidelines	See “Configure Encryption” on page 319.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

encryption-algorithm

Syntax	encryption-algorithm (3des-cbc des-cbc);
Hierarchy Level	[edit security ike], [edit security ipsec], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure an IKE or IPSec encryption algorithm.
Options	encryption-algorithm—Type of encryption algorithm. The encryption algorithm can be one of the following: 3des-cbc—Has block size of 24 bytes; its key size is 192 bits long. des-cbc—Has a block size of 8 bytes; its key size is 48 bits long.
Usage Guidelines	See “Configure an IKE Encryption Algorithm” on page 323 and “Configure an Encryption Algorithm” on page 327.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

ike

Syntax	ike { proposal <i>ike-proposal-name</i> { authentication-algorithm (md5 sha1); authentication-method pre-shared-keys; dh-group (group1 group2); encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i> ; } policy <i>ike-peer-address</i> { mode (aggressive main); proposal [<i>ike-proposal-names</i>]; pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); } }
Hierarchy Level	[edit security]
Description	Configure IKE. The statements are explained separately.
Usage Guidelines	See “Configure IKE (Dynamic SAs Only)” on page 321.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ipsec

```

Syntax ipsec {
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol esp;
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposal [ipsec-proposal-names];
    }
    security-association name {
        mode (tunnel | transport);
        replay-window-size (32 | 64);
        manual {
            direction (inbound | outbound | bi-directional) {
                spi spi-value;
                protocol (esp | ah);
                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 ipsec-policy policy-name;
        }
    }
}

```

Hierarchy Level [edit security]

Description Configure IPSec.

The statements are explained separately.

Usage Guidelines See “Configure Global IPSec Properties” on page 312.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

lifetime-seconds

Syntax	lifetime-seconds <i>seconds</i> ;
Hierarchy Level	[edit security ike], [edit security ipsec], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	(Optional) Configure lifetime of IKE or IPSec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.
Options	<i>seconds</i> —lifetime in seconds. Range: 180 through 4,294,967,295
Usage Guidelines	See “Configure IKE Lifetime” on page 323 and “Configure IPSec Lifetime” on page 328.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

manual

Syntax	<pre> manual { direction (inbound outbound bi-directional) { spi <i>spi-value</i>; protocol (esp ah); authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } } } </pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define a manual IPSec SA. The remaining statements are explained separately.
Usage Guidelines	See “Configure a Manual Security Association” on page 316.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

mode

mode (IPSec)

Syntax	mode (transport tunnel);
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define the mode for the IPSec security association.
Options	mode—Type of IPSec protection. transport—Protects host-to-host connections. tunnel—Protects traffic traveling between two security gateways. Default: tunnel

**Note**

Tunnel mode requires the ES PIC.

The JUNOS software supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the JUNOS software does not support AH and ESP header bundles.

Usage Guidelines	See “Configure IPSec Mode” on page 315.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

mode (IKE)

Syntax	mode (aggressive main);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define IKE policy mode.
Options	mode—Type of IKE policy. aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. main—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection. Default: main
Usage Guidelines	See “Configure IKE Policy Mode” on page 325.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

perfect-forward-secrecy

Syntax perfect-forward-secrecy {
 keys (group1 | group2);
 }

Hierarchy Level [edit security ipsec policy *ipsec-policy-name*]

Description (Optional) Define Perfect Forward Secrecy (PFS). Creates single use keys.

Options keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.

The key can be one of the following:

group1—768-bit.

group2—1,024-bit.

Usage Guidelines See “Configure Perfect Forward Secrecy” on page 329.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

policy

policy (IPSec)

Syntax policy *ipsec-policy-name* {
 perfect-forward-secrecy {
 keys (group1 | group2);
 }
 proposal [*ipsec-proposal-names*];
 }

Hierarchy Level [edit security ipsec]

Description Define an IPSec policy.

Options *ipsec-policy-name*—Specifies a IPSec policy name.

proposal—Lists proposals to be used by the IPSec policy.

The remaining statements are explained separately.

Usage Guidelines See “Configure an IPSec Policy” on page 329.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

policy (IKE)

Syntax	<pre> policy <i>ike-peer-address</i> { mode (aggressive main); proposal [<i>ike-proposal-names</i>]; pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); } </pre>
Hierarchy Level	[edit security ike]
Description	Define an IKE policy.
Options	<p><i>ike-peer-address</i>—A tunnel address configured at the [edit interfaces es] hierarchy level.</p> <p><i>proposal</i>—Lists proposals to be used by IKE policy.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configure an IKE Policy” on page 324.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

pre-shared-key

Syntax	pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define a preshared key for an IKE policy.
Options	<p>pre-shared-key—Type of preshared key.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none"> ascii-text—ASCII text key. hexadecimal—Hexadecimal key. <p>The preshared key can be an ACSII text or hexadecimal character key.</p>
Usage Guidelines	See “Configure IKE Policy Preshared Key” on page 325.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

- proposal

- proposal (IPSec)**

- Syntax** `proposal ipsec-proposal-name {`
`authentication-algorithm (hmac-md5-96 | hmac-sha1-96);`
`encryption-algorithm (3des-cbc | des-cbc);`
`lifetime-seconds seconds;`
`protocol esp;`
`}`

- Hierarchy Level** [edit security ipsec]

- Description** Define an IPSec proposal for a dynamic SA.

- Options** *ipsec-proposal-name*—Specifies an IPSec proposal name.

- The statements are explained separately.

- Usage Guidelines** See “Configure an IPSec Proposal” on page 327.

- Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

- proposal (IKE)**

- Syntax** `proposal ike-proposal-name {`
`authentication-algorithm (md5 | sha1);`
`authentication-method pre-shared-keys;`
`dh-group (group1 | group2);`
`encryption-algorithm (3des-cbc | des-cbc);`
`lifetime-seconds seconds;`
`}`

- Hierarchy Level** [edit security ike]

- Description** Define an IKE proposal for a dynamic SA.

- Options** *ike-proposal-name*—Specifies a IKE proposal name

- The statements are explained separately.

- Usage Guidelines** See “Configure an IPSec Proposal” on page 327.

- Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

protocol

protocol (manual SA)

Syntax	protocol (esp ah);
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bidirectional)]
Description	Define an IPSec protocol for a manual SA.
Options	protocol—Type of IPSec protocol The protocol can be one of the following: esp—Encapsulating security payload protocol. ah—Authentication header protocol.
Usage Guidelines	See “Configure the Protocol” on page 317.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

protocol (dynamic SA)

Syntax	protocol esp;
Hierarchy Level	[edit security ipsec], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Define an IPSec protocol for a dynamic SA.
Options	esp—Encapsulating security payload (the tunnel statement must be included at the [edit security ipsec security-association <i>name</i> mode] hierarchy level).

**Note**

The JUNOS software does not support the Authentication Header protocol in tunnel mode.

Usage Guidelines	See “Configure Protocol for Dynamic SA” on page 328.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

replay-window-size

Syntax	replay-window-size (32 64);
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Configure antireplay protection window size.
Options	replay-window-size—Antireplay window size. 32—32-packet window size. 64—64-packet window size.
Usage Guidelines	See “Configure IPSec Replay Window Size” on page 315.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

security-association

Syntax	<pre> security-association <i>name</i> { mode (tunnel transport); replay-window-size (32 64); manual { direction (inbound outbound bi-directional) { spi <i>spi-value</i>; protocol (esp ah); authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } } dynamic ipsec-policy <i>policy-name</i>; } } </pre>
Hierarchy Level	[edit security ipsec]
Options	<i>name</i> —Name of security association The remaining statements are explained separately.
Description	Configure an IPSec security association.
Usage Guidelines	See “Configure Security Associations” on page 313.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

spi

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec security-association <i>name</i> manual direction (inbound outbound bi-directional)]
Description	Configure Security Parameter Index (SPI) for an SA.
Options	<i>spi-value</i> —An arbitrary value that uniquely identifies which security association (SA) to use at the receiving host (the destination address in the packet). Range: 256 through 16, 639
Usage Guidelines	See “Configure a Security Parameter Index (SPI)” on page 318.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

