

Chapter 31

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 422.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

auxiliary-spi

- Syntax** auxiliary-spi *auxiliary-spi-value*;
- Hierarchy Level** [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional)]
- Description** Configure auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
- Options** *auxiliary-spi-value*—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 the Auxiliary Security Parameter Index” on page 421. For information about SPI, see “Configure a Security Parameter Index (SPI)” on page 421 and “spi” on page 478.
- 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 426.
- 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 <i>ipsec-proposal-name</i>]
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 431.
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 (dsa-signatures pre-shared-keys rsa-signatures);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure IKE authentication method.
Options	dsa-signatures—Digital signature algorithm (DSA). rsa-signatures—Public key algorithm (supports encryption and digital signatures). 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 426.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

ca-name

Syntax	ca-name <i>ca-identity</i> ;
Hierarchy Level	[edit security certificates certification-authority]
Description	Specifies the CA identity to use in the certificate request
Usage Guidelines	See “Specify the Certification Authority Name” on page 439.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

cache-size

Syntax cache-size *bytes*;

Hierarchy Level [edit security certificates]

Description Configures cache size for digital certificates

Options *bytes*—cache size for digital certificates
Range: 64 through 4,294,967,295



We recommend that you limit your cache size to 4MB.

Note

Usage Guidelines See “Configure the Cache Size” on page 441.

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

cache-timeout-negative

Syntax cache-timeout-negative *seconds*;

Hierarchy Level [edit security certificates]

Description Configures negative cache for digital certificates

Options *seconds*—negative time to cache digital certificates in seconds.
Range: 10 through 4,294,967,295



Configuring a large negative cache value can lead to a denial of service attack.

Note

Usage Guidelines See “Configure the Negative Cache” on page 441.

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

certificates

Syntax	cache-size <i>bytes</i> ; cache-timeout-negative <i>seconds</i> ; certification-authority <i>ca-profile-name</i> { ca-name <i>ca-identity</i> ; crl <i>file-name</i> ; encoding (binary pem); enrollment-url <i>url-name</i> ; file <i>certificate-file-name</i> ; ldap-url <i>url-name</i> ; } enrollment-retry <i>number</i> ; maximum-certificates <i>number</i> ; path-length <i>bytes</i> ;
Hierarchy Level	[edit security certificates]
Description	Configures Digital Certificates for IPSec.
Usage Guidelines	See “Digital Certificates Guidelines” on page 436.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

certification-authority

Syntax	certification-authority <i>ca-profile-name</i> { ca-name <i>ca-identity</i> ; crl <i>file-name</i> ; enrollment-url <i>url-name</i> ; file <i>certificate-file-name</i> ; ldap-url <i>url-name</i> ; } }
Hierarchy Level	[edit security certificates]
Description	Certification authority profile name. The remaining statements are explained separately.
Usage Guidelines	See “Configure the Certification Authority Properties” on page 439.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration

crl

Syntax	<code>crl file-name;</code>
Hierarchy Level	[edit security certificates]
Description	Configures the certificate revocation list (CRL). A certificate revocation list (CRL) is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
Options	<i>file-name</i> —Specifies the file to read the CRL from.
Usage Guidelines	See “Configure the Certification Authority Properties” on page 439.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration

description

Syntax	<code>description policy-description;</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Specifies a description for an IKE policy.
Usage Guidelines	See “Configure IKE Policy Description” on page 429.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

dh-group

Syntax	<code>dh-group (group1 group2);</code>
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the IKE Diffie-Hellman group.
Options	<i>dh-group</i> —Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. The value can be one of the following: group1—768 bit. group2—1,024-bit.
Usage Guidelines	See “Configure an IKE Diffie-Hellman Group” on page 426.
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 <i>name</i> manual]
Description	Define the direction of IPSec processing.
Options	inbound—Inbound SA. outbound—Outbound SA. bidirectional—Bidirectional SA.
Usage Guidelines	See “Configure Direction” on page 419.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

dynamic

Syntax	dynamic { window-replay-size (32 64); ipsec-policy <i>ipsec-policy-name</i> ; }
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define a dynamic IPSec SA.
Options	replay-window-size—Antireplay window size. The replay-window-size statement is optional. 32—32-packet window size. 64—64-packet window size. ipsec-policy <i>ipsec-policy-name</i> —Name of IPSec policy.
Usage Guidelines	See “Configure Dynamic Security Associations” on page 423 and “Configure the ES PIC” on page 447.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

• encoding

• **Syntax** encoding (binary | pem);

• **Hierarchy Level** [edit security ike policy *ike-peer-address*],
[edit security certificates certificate-authority *ca-profile-name*]

• **Description** Specifies the file format used for the local-certificate and local-key-pair statements.


• **Options** binary—Binary file format.

• pem—Privacy Enhanced Mail (PEM), an ASCII base64 encoded format.
Default: binary

• **Usage Guidelines** See “Configure the Type of Encoding Your CA Supports” on page 440 and “Configure the Type of Encoding Your CA Supports” on page 443.

• **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, we recommend that the first 8 bytes are not the same as the second 8 bytes, and the second 8 bytes are the 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 422.
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 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: <ul style="list-style-type: none"> 3des-cbc—Has a key size of 24 bytes; its key size is 192 bits long. des-cbc—Has a key size of 8 bytes; its key size is 48 bits long.
Usage Guidelines	See “Configure an IKE Encryption Algorithm” on page 427 and “Configure an Encryption Algorithm” on page 432.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

enrollment-retry

Syntax	enrollment-retry <i>number</i> ;
Hierarchy Level	[edit security certificates]
Description	Specifies how many times a router will resend a digital certificate request.
Options	<i>number</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Usage Guidelines	See “Configure the Number of Enrollment Retries” on page 442
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

enrollment-url

Syntax	enrollment-url <i>url-name</i> ;
Hierarchy Level	[edit security certificates certification-authority <i>certification-authority</i>]
Options	<i>url-name</i> —Certificate Authority URL.
Description	Specifies where your router should send SCEP based certificate enrollment requests (Certification Authority URL).
Usage Guidelines	See “Specify an Enrollment URL” on page 440.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

file

Syntax	file <i>certificate-name</i> ;
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Description	Specifies which file to read the digital certificate from.
Options	<i>certificate-name</i> —File to read the digital certificate from.
Usage Guidelines	See “Specify a File to Read the Digital Certificate” on page 440
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> { description <i>policy-description</i> ; encoding (binary pem); identity <i>identity-name</i> ; local-certificate <i>certificate-file-name</i> ; local-key-pair <i>private-public-key-file</i> ; mode (aggressive main); pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); proposal [<i>ike-proposal-names</i>]; } }
Hierarchy Level	[edit security]
Description	Configure IKE. The statements are explained separately.
Usage Guidelines	See “Configure an IKE Proposal (Dynamic SAs Only)” on page 425 and “Configure an IKE Policy for Preshared Keys” on page 428 .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

identity

Identity identity *identity-name*;

Hierarchy Level [edit security ike]

Description Defines the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).

Usage Guidelines See “Configure the Identity to Define the Remote Certificate Name” on page 444.

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

        traceoptions {
            file <files number> < size size>;
            flag all;
            flag database;
            flag general;
            flag ike;
            flag parse;
            flag policy-manager;
            flag routing-socket;
            flag timer;
        }
    }
}

```

- Hierarchy Level** [edit security]
- Description** Configure IPSec.
The statements are explained separately.
- Usage Guidelines** See “Configure Security Associations” on page 416.
- Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

ldap-url

- Syntax;** ldap-url *url-name*;
- Hierarchy Level** [edit security certificates certification-authority *certification-authority*]
- Description** (Optional) Specifies the LDAP URL for digital certificates.
- Options** *url*—name of LDAP URL.
- Usage Guidelines** See the “Specify an LDAP URL” on page 441
- 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 *seconds*;
- Hierarchy Level** [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]
- 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** *seconds*—lifetime in seconds.
Range: 180 through 86,400
- Usage Guidelines** See “Configure an IKE Lifetime” on page 427 and “Configure IPSec Lifetime” on page 432.
- Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

local

- Syntax;** local *certificate-name*;
- Hierarchy Level** [edit security certificates]
- Description** Imports an SSL certificate into the router

**Note**

Configuring xnm-ssl service does not apply to IPSec.

- Options** *certificate-name*—SSL certificate name.
- Usage Guidelines** See “JUNOScript XNM-SSL Service” on page 453.

local-key-pair

- Syntax;** local-key-pair *private-public-key-file*;
- Hierarchy Level** [edit security ike policy *ike-peer-address*]
- Description** Specify private and public keys.
- Options** *certificate-file-name*—Specifies the file from which to read the private and public key pair.
- Usage Guidelines** See “Specify the Private and Public Key File” on page 444.
- Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

manual

```

Syntax  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);
                }
            }
        }

```

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

Description Define a manual IPSec SA.

The remaining statements are explained separately.

Usage Guidelines See “Configure Manual Security Associations” on page 419.

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

maximum-certificates

```

Syntax  maximum-certificates number;

```

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Description Configures the maximum number of peer digital certificates to be cached.

Options *number*—Maximum number of peer digital certificates to be cached.

Range: 64 through 4,294,967,295 peer certificates

Default: 1,024 peer certificates

Usage Guidelines See “Configure the Maximum Number of Peer Certificates” on page 442.

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

mode

mode (IPSec)**Syntax** mode (transport | tunnel);**Hierarchy Level** [edit security ipsec security-association *name*]**Description** Define the mode for the IPSec security association.**Options** transport— Protects traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. VPN gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications.

tunnel—Protects traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.

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.

In transport mode, the JUNOS software supports only BGP.

Usage Guidelines See “Configure IPSec Mode” on page 417.**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 429.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

path-length

Syntax	path-length <i>certificate-path-length</i> ;
Hierarchy Level	[edit security certificates]
Description	Configures the digital certificate path length.
Options	<i>certificate-path-length</i> —Digital certificate path length. Range: 2 through 15 certificates Default: 15 certificates
Usage Guidelines	See “Configure the Path Length for the Certificate Hierarchy” on page 442.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

perfect-forward-secrecy

Syntax	perfect-forward-secrecy { keys (group1 group2); }
Hierarchy Level	[edit security ipsec policy <i>ipsec-policy-name</i>]
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 434.
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 <i>ipsec-policy-name</i> { perfect-forward-secrecy { keys (group1 group2); } proposal [<i>ipsec-proposal-names</i>]; }
Hierarchy Level	[edit security ipsec]
Description	Define an IPSec policy.
Options	<i>ipsec-policy-name</i> —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 433.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

policy (IKE)

Syntax `policy ike-peer-address {
 description policy-description;
 encoding (binary | pem);
 identity identity-name;
 local-certificate certificate-file-name;
 local-key-pair private-public-key-file;
 mode (aggressive | main);
 proposal [ike-proposal-names];
 pre-shared-key (ascii-text key | hexadecimal key);
}`

Hierarchy Level [edit security ike]

Description Define an IKE policy.

Options *ike-peer-address*—A tunnel address configured at the [edit interfaces es] hierarchy level.
proposal—Names of proposals to be used by the IKE policy.
 The remaining statements are explained separately.

Usage Guidelines See “Configure an IKE Policy for Preshared Keys” on page 428.

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

pre-shared-key

Syntax `pre-shared-key (ascii-text key | hexadecimal key);`

Hierarchy Level [edit security ike policy *ike-peer-address*]

Description Define a preshared key for an IKE policy.

Options *preshared-key*—Type of preshared key.

The key can be one of the following:

ascii-text—ASCII text key.

hexadecimal—Hexadecimal key.

The preshared key can be an ACSII text or hexadecimal character key.

Usage Guidelines See “Configure IKE Policy Preshared Key” on page 429.

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

proposal

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 remaining statements are explained separately.

Usage Guidelines See “Configure an IKE Proposal (Dynamic SAs Only)” on page 425.

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

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 (ah | esp | bundle);
 }`

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 431.

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

security-association

```

Syntax 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;
        }
    }
}

```

Hierarchy Level [edit security ipsec]

Options *name*—Name of security association

The remaining statements are explained separately.

Description Configure an IPSec security association.

Usage Guidelines See “Configure Security Associations” on page 416.

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

spi

Syntax `spi spi-value;`

Hierarchy Level [edit security ipsec security-association *name* manual direction (inbound | outbound | bi-directional)]

Description Configure Security Parameter Index (SPI) for an SA.

Options *spi-value*—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.



Note

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

Usage Guidelines See “Configure a Security Parameter Index (SPI)” on page 421.

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

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>>; flag all; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; } </pre>
Hierarchy Level	[edit security]
Description	<p>Configure security tracing options.</p> <p>To specify more than one tracing option, include multiple flag statements. The output of the security tracing options is placed in one file: /var/log/kmd.</p>
Options	<p><i>files number</i>—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p><i>size size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, kmd) reaches this size, it is renamed, kmd.0, then kmd.1 and so on., until the maximum number of trace files is reached. Then the oldest trace file is overwritten. Default: 1024 KB</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option: Range: 2 through 1,000 files Default: 10 files</p> <p><i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <p>all—Trace all security event</p> <p>database—Trace database events</p> <p>general—Trace general events</p> <p>ike—Trace IKE module processing</p> <p>parse—Trace configuration processing</p> <p>policy-manager—Trace policy manager processing</p> <p>routing-socket—Trace routing socket messages</p> <p>timer—Trace internal timer events</p>

