

Chapter 13

Summary of IPSec Services Configuration Statements

The following sections explain each of the Internet Protocol Security (IPSec) services statements. The statements are organized alphabetically.

authentication

Syntax	authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); }
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then manual direction <i>direction</i>]
Description	Configure IPSec authentication parameters for manual SA.
Options	algorithm—Hash algorithm that authenticates packet data. The algorithm can be one of the following: hmac-md5-96—Produces a 128-bit digest. hmac-sha1-96—Produces a 160-bit digest. key—Type of authentication key. The key can be one of the following: 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 “Configuring Authentication” on page 118.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm

See the following sections:

authentication-algorithm (IKE) on page 140

authentication-algorithm (IPSec) on page 140

authentication-algorithm (IKE)

Syntax	authentication-algorithm (md5 sha1);
Hierarchy Level	[edit services ipsec-vpn ike proposal <i>proposal-name</i>]
Description	Configure the IKE hash algorithm that authenticates packet data.
Options	md5—Produces a 128-bit digest. sha1—Produces a 160-bit digest.
Usage Guidelines	See “Configuring an IKE Authentication Algorithm” on page 121.
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 services ipsec-vpn ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure the IPSec hash algorithm that authenticates packet data.
Options	hmac-md5-96—Produces a 128-bit digest. hmac-sha1-96—Produces a 160-bit digest.
Usage Guidelines	See “Configuring an Authentication Algorithm” on page 126.
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 services ipsec-vpn ike proposal <i>proposal-name</i>]
Description	Configure an 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 “Configuring an IKE Authentication Method” on page 121.
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 <i>spi-value</i> ;
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then manual direction <i>direction</i>]
Description	Configure an auxiliary Security Parameter Index (SPI) for a manual security association (SA). Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
Options	<i>spi-value</i> —An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet). Range: 256 through 16,639
Usage Guidelines	See “Configuring the Auxiliary Security Parameter Index” on page 117. For information about SPI, see “Configuring the Security Parameter Index” on page 117 and “spi” on page 159.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

backup-remote-gateway

Syntax	backup-remote-gateway <i>address</i> ;
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then]
Description	Define the backup remote address to which the IPSec traffic is directed when the primary remote gateway is down. Configuring this statement also enables the dead peer detection (DPD) protocol.
Options	<i>address</i> —Backup remote address.
Usage Guidelines	See “Configuring IPSec Actions” on page 133.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

clear-dont-fragment-bit

Syntax	clear-dont-fragment-bit;
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]
Description	Clear the Don't Fragment (DF) bit on all IPv4 packets entering the IPSec tunnel. If the encapsulated packet size exceeds the tunnel MTU, the packet is fragmented before encapsulation.
Usage Guidelines	See “Configuring IPSec Actions” on page 133.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

description

Syntax	description <i>description</i> ;
Hierarchy Level	[edit services ipsec-vpn ike policy <i>policy-name</i>], [edit services ipsec-vpn ike proposal <i>proposal-name</i>], [edit services ipsec-vpn ipsec policy <i>policy-name</i>], [edit services ipsec-vpn ipsec proposal <i>proposal-name</i>]
Description	Specify the text description for an IKE or IPSec policy or proposal.
Usage Guidelines	See “Configuring an IKE Policy Description” on page 124.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

destination-address

Syntax	destination-address <i>address</i> ;
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> from]
Description	Specify the destination address for rule matching.
Options	<i>address</i> —Destination IP address.
Usage Guidelines	See “Configuring IPSec Match Conditions” on page 133.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

dh-group

Syntax	dh-group (group1 group2);
Hierarchy Level	[edit services ipsec-vpn ike proposal <i>proposal-name</i>]
Description	Configure the IKE Diffie-Hellman prime modulus group to use for performing the new Diffie-Hellman exchange.
Options	group1—768-bit. group2—1024-bit.
Usage Guidelines	See “Configuring an IKE Diffie-Hellman Group” on page 121.
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) {
 protocol (ah | bundle | esp);
 spi *spi-value*;
 auxiliary-spi *spi-value*;
 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 services ipsec-vpn rule *rule-name* term *term-name* then manual]

Description Specify the direction in which manual security associations (SAs) are applied.

Options bidirectional—Apply the SA in both directions.
 inbound—Apply the SA on inbound traffic.
 outbound—Apply the SA on outbound traffic.

Usage Guidelines See “Configuring IPsec Rule Content” on page 132.

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

dynamic

Syntax dynamic {
 ike-policy *policy-name*;
 ipsec-policy *policy-name*;
 }

Hierarchy Level [edit services ipsec-vpn match-direction *rule-name* term *term-name* then]

Description Define a dynamic IPsec SA.


Options ike-policy *policy-name*—Name of the IKE policy. This statement is optional for the non-preshared-key authentication method. For digital signature-based authentication, this statement is optional and the default policy is used if none is supplied.

ipsec-policy *policy-name*—Name of the IPsec policy. This statement is optional and the default policy is used if none is supplied.

Usage Guidelines See “Configuring Dynamic Security Associations” on page 119.

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

encryption

Syntax	encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); }
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then manual direction <i>direction</i>]
Description	Configure an encryption algorithm and key for manual SA.
Options	algorithm—Type of encryption algorithm. The algorithm can be one of the following: des-cbc—Has a block size of 8 bytes (64 bits); the key size is 48 bits long. 3des-cbc—Has a block size of 8 bytes (64 bits); the key size is 192 bits long.
	NOTE: For 3des-cbc, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.
	key—Type of encryption key. The key can be one of the following: 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 3des-cbc, the key contains 48 hexadecimal characters.
Usage Guidelines	See “Configuring Encryption” on page 118.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

encryption-algorithm

Syntax	encryption-algorithm (3des-cbc des-cbc);
Hierarchy Level	[edit services ipsec-vpn ike proposal <i>proposal-name</i>], [edit services ipsec-vpn ipsec proposal <i>proposal-name</i>]
Description	Configure an IKE or IPSec encryption algorithm.
Options	3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long. des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.
Usage Guidelines	See “Configuring an IKE Encryption Algorithm” on page 122 and “Configuring an Encryption Algorithm” on page 127.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

from

Syntax	from { destination-address <i>address</i> ; source-address <i>address</i> ; }
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i>]
Description	Specify input conditions for the IPsec term.
Options	For information on match conditions, see the description of firewall filter match conditions in the <i>JUNOS Policy Framework Configuration Guide</i> . The remaining statements are explained separately.
Usage Guidelines	See “Configuring IPsec Rule Content” on page 132.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ike

```

Syntax  ike {
            proposal proposal-name {
                authentication-algorithm (md5 | sha1);
                authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
                description description;
                dh-group (group1 | group2);
                encryption-algorithm (3des-cbc | des-cbc);
                lifetime-seconds seconds;
            }
            policy policy-name {
                description description;
                local-id {
                    ipv4_addr [ values ];
                    key_id [ values ];
                }
                mode (aggressive | main);
                pre-shared-key (ascii-text key | hexadecimal key);
                proposals [ proposal-names ];
                remote-id {
                    ipv4_addr [ values ];
                    key_id [ values ];
                }
            }
        }

```

Hierarchy Level [edit services ipsec-vpn]

Description Configure IKE.

The statements are explained separately.

Usage Guidelines See “Configuring an IKE Proposal” on page 120 and “Configuring an IKE Policy for Preshared Keys” on page 122.

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

ipsec

Syntax	<pre> ipsec { proposal <i>proposal-name</i> { authentication-algorithm (hmac-md5-96 hmac-sha1-96); description <i>description</i>; encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i>; protocol (ah esp bundle); } policy <i>policy-name</i> { description <i>description</i>; perfect-forward-secrecy { keys (group1 group2); } proposals [<i>proposal-names</i>]; } } </pre>
Hierarchy Level	[edit services ipsec-vpn]
Description	<p>Configure IPSec.</p> <p>The statements are explained separately.</p>
Usage Guidelines	See “Configuring Security Associations” on page 114.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

lifetime-seconds

Syntax;	lifetime-seconds <i>seconds</i> ;
Hierarchy Level	[edit services ipsec-vpn ike proposal <i>proposal-name</i>], [edit services ipsec-vpn ipsec proposal <i>proposal-name</i>]
Description	Configure the lifetime of an IKE or IPSec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated. This statement is optional.
Options	<p><i>seconds</i>—Lifetime, in seconds.</p> <p>Range: 180 through 86,400</p>
Usage Guidelines	See “Configuring an IKE Lifetime” on page 122 and “Configuring the IPSec Lifetime” on page 127.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

local-id

Syntax;	local-id { ipv4_addr [<i>values</i>]; key_id [<i>values</i>]; }
Hierarchy Level	[edit services ike policy <i>policy-name</i>]
Description	Specify local identifiers for IKE Phase 1 negotiation. This statement is optional.
Options	ipv4_addr [<i>values</i>]—Define one or more IPv4 address identification values. key_id [<i>values</i>]—Define one or more key identification values.
Usage Guidelines	See “Configuring Local and Remote IDs” on page 124.
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 bidirectional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } auxiliary-spi <i>spi-value</i> ; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } spi <i>spi-value</i> ; protocol (ah esp bundle); } }
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then]
Description	Define a manual IPSec SA. The remaining statements are explained separately.
Usage Guidelines	See “Configuring Manual Security Associations” on page 115.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

match-direction

Syntax	match-direction (input output);
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i>]
Description	Specify the direction in which the rule match is applied.
Options	input—Apply the rule match on input. output—Apply the rule match on input.
Usage Guidelines	See “Configuring IPSec Rule Content” on page 132.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

mode

Syntax	mode (aggressive main);
Hierarchy Level	[edit services ipsec-vpn ike policy <i>policy-name</i>]
Description	Define an IKE policy mode.
Options	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 “Configuring the IKE Policy Mode” on page 123.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

no-anti-replay

Syntax	no-anti-replay;
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then]
Description	Disable IPSec anti-replay service, which occasionally causes interoperability issues for security associations.
Usage Guidelines	See “Disabling Anti-Replay” on page 135.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

perfect-forward-secretcy

Syntax	perfect-forward-secretcy { keys (group1 group2); }
Hierarchy Level	[edit services ipsec-vpn ipsec policy <i>policy-name</i>]
Description	Define Perfect Forward Secrecy (PFS). Creates single-use keys. This statement is optional.
Options	<p>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:</p> <p> group1—768-bit.</p> <p> group2—1024-bit.</p>
Usage Guidelines	See “Configuring Perfect Forward Secrecy” on page 129.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

policy

See the following sections:

policy (IKE) on page 152

policy (IPSec) on page 152

policy (IKE)

Syntax `policy policy-name {
 description description;
 local-id {
 ipv4_addr [values];
 key_id [values];
 }
 mode (aggressive | main);
 pre-shared-key (ascii-text key | hexadecimal key);
 proposals [proposal-names];
 remote-id {
 ipv4_addr [values];
 key_id [values];
 }
}`

Hierarchy Level [edit services ike]

Description Define an IKE policy.

Options *policy-name*—Specifies an IKE policy name.

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IKE Policy for Preshared Keys” on page 122.

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

policy (IPSec)

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

Hierarchy Level [edit services ipsec-vpn ipsec]

Description Define an IPSec policy.

Options *policy-name*—Specifies an IPSec policy name.

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IPSec Policy” on page 128.

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 services ike policy *policy-name*]

Description Define a preshared key for an IKE policy.

Options *key*—Value of preshared key. The key can be one of the following:

ascii-text—ASCII text key.

hexadecimal—Hexadecimal key.

Usage Guidelines See “Configuring an IKE Policy for Preshared Keys” on page 122.

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

proposal

See the following sections:

proposal (IKE) on page 154

proposal (IPSec) on page 154

proposal (IKE)

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

Hierarchy Level [edit services ipsec-vpn ike]

Description Define an IKE proposal for a dynamic SA.

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

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IKE Proposal” on page 120.

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

proposal (IPSec)

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

Hierarchy Level [edit services ipsec-vpn ipsec]

Description Define an IPSec proposal for a dynamic SA.

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

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IPSec Proposal” on page 126.

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

proposals

Syntax	<code>proposals [<i>proposal-names</i>];</code>
Hierarchy Level	[edit services ipsec-vpn ike policy <i>policy-name</i>], [edit services ipsec-vpn ipsec policy <i>policy-name</i>]
Description	Define a list of proposals to include in the IKE or IPSec policy.
Options	<i>proposal-names</i> —List of IKE or IPSec proposal names.
Usage Guidelines	See “Configuring an IKE Proposal” on page 120.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

protocol

Syntax	<code>protocol (ah esp bundle);</code>
Hierarchy Level	[edit services ipsec-vpn ipsec proposal <i>proposal-name</i>], [edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then manual direction <i>direction</i>]
Description	Define an IPSec protocol for a dynamic or manual SA.
Options	ah—Authentication Header protocol. esp—Encapsulating Security Payload protocol. bundle—AH and ESP protocol.
Usage Guidelines	See “Configuring the Protocol” on page 116.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

remote-gateway

Syntax	<code>remote-gateway <i>address</i>;</code>
Hierarchy Level	[edit services ipsec-vpn match-direction <i>rule-name</i> term <i>term-name</i> then]
Description	Define the remote address to which the IPSec traffic is directed.
Options	<i>address</i> —Remote address.
Usage Guidelines	See “Configuring IPSec Actions” on page 133.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

remote-id

Syntax	<pre>remote-id { ipv4_addr [values]; key_id [values]; }</pre>
Hierarchy Level	[edit services ipsec-vpn ike policy <i>policy-name</i>]
Description	Define the remote identification values to which the IKE policy applies.
Options	<p>ipv4_addr [<i>values</i>]—Define one or more IPv4 address identification values.</p> <p>key_id [<i>values</i>]—Define one or more key identification values.</p>
Usage Guidelines	See “Configuring the Protocol” on page 116.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

rule

```

Syntax rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
            destination-address address;
            source-address address;
        }
        then {
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm (des-cbc | 3des-cbc);
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            clear-dont-fragment-bit;
            remote-gateway address;
            syslog;
        }
    }
}

```

Hierarchy Level [edit services ipsec-vpn],
[edit services ipsec-vpn rule-set *rule-set-name*]

Description Specify the rule the router uses when applying this service.

Options *rule-name*—Identifier for the collection of terms that comprise this rule.

The remaining statements are explained separately.

Usage Guidelines See “Configuring IPSec Rule Content” on page 132.

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

rule-set

Syntax	<code>rule-set <i>rule-set-name</i> { [rule <i>rule-names</i>]; }</code>
Hierarchy Level	[edit services ipsec-vpn]
Description	Specify the rule set the router uses when applying this service.
Options	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
Usage Guidelines	See “Configuring the IPSec Rule Set” on page 131.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.


services

Syntax	<code>services ipsec-vpn { ... }</code>
Hierarchy Level	[edit]
Description	Define the service rules to be applied to traffic.
Options	ipsec-vpn—Identifies the IPSec set of rules statements.
Usage Guidelines	See “IPSec Services Configuration Guidelines” on page 111.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address

Syntax	<code>source-address <i>address</i>;</code>
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> from]
Description	Specify the source address for rule matching.
Options	<i>address</i> —Source IP address.
Usage Guidelines	See “Configuring IPSec Match Conditions” on page 133.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

spi

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then manual direction <i>direction</i>]
Description	Configure the 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
	NOTE: Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
Usage Guidelines	See “Configuring the Security Parameter Index” on page 117.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

syslog

Syntax	<code>syslog;</code>
Hierarchy Level	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]
Description	Enable system logging. The system log information of the Adaptive Services PIC is passed to the kernel for logging in the /var/log directory.
Usage Guidelines	See “Configuring IPSec Actions” on page 133.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

term

```

Syntax term term-name {
    from {
        destination-address address;
        source-address address;
    }
    then {
        dynamic {
            ike-policy policy-name;
            ipsec-policy policy-name;
        }
        manual {
            direction (inbound | outbound | bidirectional) {
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi spi-value;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
                protocol (ah | bundle | esp);
                spi spi-value;
            }
        }
        clear-dont-fragment-bit;
        remote-gateway address;
        syslog;
    }
}

```

Hierarchy Level [edit services ipsec-vpn rule *rule-name*]

Description Define the IPSec term properties.

Options *term-name*—Identifier for the term.

The remaining statements are explained separately.

Usage Guidelines See “Configuring IPSec Rule Content” on page 132.

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

then

```

Syntax  then {
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm (des-cbc | 3des-cbc);
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            clear-dont-fragment-bit;
            remote-gateway address;
            syslog;
        }

```

Hierarchy Level [edit services ipsec-vpn rule *rule-name* term *term-name*]

Description Define the IPSec term actions.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring IPSec Rule Content” on page 132.

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

