CHAPTER 25

Overview of the IPSec VPN SPA

This chapter provides an overview of the release history, feature, and Management Information Base (MIB) support for the IPSec VPN SPAs.

This chapter includes the following sections:

Release History

Release	Modification
Cisco IOS Release 15.1(3)S1	Support for WS-IPSEC-3 SPA was added on the WS-SSC-600 line card on Cisco 7600 series router.

Cisco IOS Release 12.2(33)SRA	For the IPSec VPN SPA, SPA-IPSEC-2G, the following changes were introduced: • The following features were newly introduced : – Front-side VRF – IPSec Virtual Tunnel Interface (VTI) – Certificate to ISAKMP Profile Mapping – Call Admission Control – Periodic Message Option (now supported in Dead Peer Detection) – Reverse Route Injection (RRI) – IPSec Anti-replay window size – IPSec Preferred Peer – Local Certificate Storage Location – Persistent Self-signed Certificates – Easy VPN Remote RSA Signature Storage – IPSec and IKE MIB support for Cisco VRF-Aware IPSec • Tunnel capacity has been increased to 16,000 tunnels. • Support has been added for the following commands: – clear crypto engine accelerator counter command—To clear platform and network interface controller statistics. – show crypto engine accelerator statistic command—To display platform and network interface controller statistics. – **show crypto eli** command— To display how many IKE-SAs and IPSec sessions are active and how many Diffie-Hellman keys are in use for each IPSec VPN SPA. • Cisco IOS Release 12.2(33)SRA is only supported on Supervisor Engine 32 and Supervisor Engine 720. • Unlike previous releases, support is not included for IPSec stateful failover using HSRP and SSP. • The **crypto engine subslot** command has been replaced by the **crypto engine slot** command. • The one large configuration chapter has been restructured into several smaller chapters, and a table has been added that describes release-dependent features. • The "IPSec Feature Support in VRF Mode for SPA-IPSEC-2G IPSEC VPN SPA" has been expanded to include tables that differentiate Supervisor and line card support by release.
Cisco IOS Release 12.2(18)SXF6	For the SPA-IPSEC-2G IPSec VPN SPA, support was introduced for the IPSec anti-replay window size feature in the SX release train.
Cisco IOS Release 12.2(18)SXF2	For the SPA-IPSEC-2G IPSec VPN SPA , support was introduced for Supervisor Engine 2, Supervisor Engine 32, and the configuration of IP multicast over a GRE tunnel.

Cisco IOS Release 12.2(18)SXE5	For the SPA-IPSEC-2G IPSec VPN SPA, support was introduced for two new GRE takeover commands: • **crypto engine gre supervisor** command—To configure the router to process Generic Routing Encapsulation (GRE) using the Supervisor Engine hardware or the Route Processor (RP). • **crypto engine gre vpnblade** command—To configure the router to process Generic Routing Encapsulation (GRE) using the IPSec VPN SPA.
Cisco IOS Release 12.2(18)SXE2	For the SPA-IPSEC-2G IPSec VPN SPA, support was introduced on the Cisco 7600 SSC-400 on the Cisco 7600 series router.

Overview of the IPSec VPN SPAs

The IPSec VPN SPAs are Gigabit Ethernet IP Security (IPSec) cryptographic SPAs that you can install in a Cisco 7600 series router to provide hardware acceleration for IPSec encryption and decryption, generic routing encapsulation (GRE), and Internet Key Exchange (IKE) key generation.

The IPSec SPAs come in the following models:

- SPA-IPSEC-2G
- WS-IPSEC-3

The SPA-IPSEC-2G SPA was introduced in Cisco IOS release 12.2(18)SXE2 and supported on the Cisco SSC 400 line card. It is a 2 Gbps IPSec VPN SPA.

The WS-IPSEC-3 SPA is a 5 Gbps VPN Service Port Adapter (VSPA) introduced in Cisco IOS release 15.1(3)S1, on the Cisco 7600 platform. This SPA should be installed on a WS-SSC-600 line card before it can be used on the Cisco 7600 series router.

Note Software-based IPSec features are not supported in any Cisco IOS releases that support the IPSec VPN SPA.

The traditional software-based implementation of IPSec in Cisco IOS supports the entire suite of security protocols including Authentication Header (AH), Encapsulating Security Payload (ESP), and IKE. The resources consumed by these activities are significant and make it difficult to achieve line-rate transmission speeds over secure virtual private networks (VPNs). To address this problem, certain platforms with large VPN bandwidth requirements support bump-in-the-wire (BITW) IPSec hardware modules in conjunction with the hardware forwarding engines. These modules off-load policy enforcement, as well as bulk encryption and forwarding, from the route processor (RP) so that it is not required to look at each packet coming through the router. This frees up resources that can be used for session establishment, key management, and other features. The IPSec VPN SPA provides a bump-in-the-wire (BITW) IPSec implementation using virtual LANs (VLANs) for a Cisco 7600 series router.

Note BITW is an IPSec implementation that starts egress packet processing after the IP stack has finished with the packet and completes ingress packet processing before the IP stack receives the packet.

The IPSec VPN SPA can use multiple Fast Ethernet or Gigabit Ethernet ports on other Cisco 7600 series router modules to connect to the Internet through WAN routers. The physical ports may be attached to the IPSec VPN SPA through a VLAN called the port-VLAN (or pvlan). Packets that are received from the WAN routers pass through the IPSec VPN SPA for IPSec processing. The packets are output on a dedicated VLAN called the interface or inside VLAN (or ivlan). Depending on the configuration mode (VRF mode or crypto-connect mode), the ivlan or pvlan may be configured explicitly or may be allocated implicitly by the system.

On the LAN side, traffic between the LAN ports can be routed or bridged on multiple Fast Ethernet or Gigabit Ethernet ports. Because the LAN traffic is not encrypted or decrypted, it does not pass through the IPSec VPN SPA.

The IPSec VPN SPA does not maintain routing information, route, or change the MAC header of a packet (except for the VLAN ID from one VLAN to another).

Note GRE over IPSec over MPLS (GREoIPSecoMPLS) through a loopback cable is not supported on the Cisco 7600 series router.

Overview of Basic IPSec and IKE Configuration Concepts

This subsection reviews some basic IPSec and IKE concepts that are used throughout the configuration of the IPSec VPN SPA, such as security associations (SAs), access lists (ACLs), crypto maps, transform sets, and IKE policies. The information presented here is introductory and should not be considered complete.

Note For more detailed information on IPSec and IKE concepts and procedures, refer to the *Cisco IOS Security Configuration Guide.*

Information About IPSec Configuration

IPSec provides secure tunnels between two peers, such as two routers. More accurately, these tunnels are sets of security associations (SAs) that are established between two IPSec peers. The SAs define which protocols and algorithms should be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (Authentication Header (AH) or Encapsulating Security Payload (ESP)). Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of SAs. For example, some data streams might be authenticated only while other data streams must both be encrypted and authenticated.

Note The use of the term “tunnel” in this subsection does not refer to using IPSec in tunnel mode.

With IPSec, you define what traffic should be protected between two IPSec peers by configuring ACLs and applying these ACLs to interfaces by way of crypto maps. (The ACLs used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate ACLs define blocking and permitting at the interface.)

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you must create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries, which specify different IPSec policies.

Crypto ACLs associated with IPSec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new SAs (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic in order to filter out and discard traffic that should have been protected by IPSec.

- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. Negotiation is performed only for ipsec-isakmp crypto map entries. In order to be accepted, if the peer initiates the IPSec negotiation, it must specify a data flow that is “permitted” by a crypto ACL associated with an ipsec-isakmp crypto map entry.

Note ACLs applied to a crypto map also known as crypto ACLs are different from normal extended ip access-lists and do NOT provide or support logging.

Crypto map entries created for IPSec combine the various parts used to set up IPSec SAs, including:

- Which traffic should be protected by IPSec (per a crypto ACL)
- The granularity of the flow to be protected by a set of SAs
- Where IPSec-protected traffic should be sent (the name of the remote IPSec peer)
- The local address to be used for the IPSec traffic
- What IPSec SA should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether SAs are manually established or are established via IKE
- Other parameters that might be necessary to define an IPSec SA

Crypto map entries are searched in order—the router attempts to match the packet to the access list specified in that entry.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peers’ IPSec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

Note To minimize the possibility of packet loss during rekeying, we recommend using time-based rather than volume-based IPSec SA expiration. By setting the lifetime volume to the maximum value using the **set security-association lifetime kilobytes 536870912** command, you can usually force time-based SA expiration.

Information About IKE Configuration

IKE is a key management protocol standard that is used in conjunction with the IPSec standard.

IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

In Cisco IOS Release 12.2(33)SXF and earlier releases, IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is enabled by default.

You configure IKE by creating IKE policies at each peer using the **crypto isakmp policy** command. An IKE policy defines a combination of security parameters to be used during the IKE negotiation and mandates how the peers are authenticated.

You can create multiple IKE policies, each with a different combination of parameter values, but at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

If you do not configure any policies, your router uses the default policy, which is always set to the lowest priority, and which contains each parameter's default value.

There are five parameters to define in each IKE policy:

- Encryption algorithm
- Hash algorithm
- Authentication method
- Diffie-Hellman group identifier
- Security association lifetime

For more information about IKE, see the "Overview of IKE" section on page 29-2.

Configuring VPNs with the IPSec VPN SPAs

To configure a VPN using the IPSec VPN SPA, you have two basic options: crypto-connect mode or Virtual Routing and Forwarding (VRF) mode. In either mode, you may also configure GRE tunneling to encapsulate a wide variety of protocol packet types, including multicast packets, inside the VPN tunnel.

Note Switching between crypto-connect mode and VRF mode requires a reload.

Note We recommend that you do not make changes to the VPN configuration while VPN sessions are active. To avoid system disruption, we recommend that you plan a scheduled maintenance time and clear all VPN sessions using the **clear crypto sessions** command before making VPN configuration changes.

Crypto-Connect Mode

Traditionally, VPNs are configured on the IPSec VPN SPA by attaching crypto maps to interface VLANs and then crypto-connecting a physical port to the interface VLAN. This method, known as crypto-connect mode, is similar to the method used to configure VPNs on routers running Cisco IOS software. When you configure VPNs on the IPSec VPN SPA using crypto-connect mode, you attach crypto maps to VLANs (using interface VLANs); when you configure VPNs on routers running Cisco IOS software, you configure individual interfaces.

Note With the IPSec VPN SPA, crypto maps are attached to individual interfaces but the set of interfaces allowed is restricted to interface VLANs.

Crypto-connect mode VPN configuration is described in Chapter 26, "Configuring VPNs in Crypto-Connect Mode."

VRF Mode

VRF mode, also known as VRF-aware IPSec, allows you to map IPSec tunnels to VPN routing and forwarding instances (VRFs) using a single public-facing address. A VRF instance is a per-VPN routing information repository that defines the VPN membership of a customer site attached to the Provider Edge (PE) router. A VRF comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

When you configure a VPN on the IPSec VPN SPA using VRF mode, the model of interface VLANs is preserved, but the **crypto connect vlan** command is not used. Instead, a route must be installed so that packets destined for that particular subnet in that particular VRF are directed to that interface VLAN.

When configuring a VPN using VRF mode, you have these additional tunneling options: tunnel protection (TP) using GRE, and Virtual Tunnel Interface (VTI). With either of these options, you can terminate tunnels in VRFs (normal VRF mode) or in the global context.

VRF mode VPN configuration is described in Chapter 27, "Configuring VPNs in VRF Mode."

IPSec Feature Support

The tables in the following sections display supported and unsupported IPSec features of the IPsec VPN Module in each VPN mode according to the software release:

- IPSec Features Common To All VPN Modes, page 25-9
- IPSec Features in Crypto-Connect Mode, page 25-17
- IPSec Features in VRF Mode, page 25-18

Note This document describes IPSec VPN SPA features and applications that have been tested and are supported. Features and applications that do not explicitly appear in this table and in the following chapters should be considered unsupported. Contact your Cisco account team before implementing a configuration that is not described in this document.

IPSec Features Common To All VPN Modes

Table 25-1 lists the supported and unsupported IPSec features common to all VPN modes for IPSec VPN SPA, SPA-IPSEC-2G.

Table 25-1 IPSec Feature Support By Release in All VPN Modes for SPA-IPSEC-2G

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Release 15S
	SXE	**SXF**	**SRA**	**SRB, SRC,** SRD,SRE	**SXH**[1]	15.0 (1)S and later
IPSec tunnels using software crypto	N	N	N	N	N	N
Enhanced GRE takeover (if the supervisor engine cannot process)	Y	Y	Y	Y	Y	Y
Multicast over GRE	N	Y	Y	Y	Y	Y
Multicast over multipoint GRE (mGRE) / DMVPN	N	N	N	N	N	N
Multicast Scalability Enhancement (single SPA mode)	N	Y	Y	Y	Y	Y
Advanced Encryption Standard (AES)	Y	Y	Y	Y	Y	Y
ISAKMP keyring	Y	Y	Y	Y	Y	Y
SafeNet Client support	Y	Y	Y	Y	Y	Y
Peer filtering (SafeNet Client support)	N	N	N	N	N	N
Certificate to ISAKMP profile mapping	Y	Y	Y	Y	Y	Y
Encrypted preshared key	Y	Y	Y	Y	Y	Y
IKE Aggressive Mode Initiation	N	N	N	N	N	N
Call Admission Control (CAC) for IKE	N	N	Y	Y	Y	Y
Dead Peer Detection (DPD) on-demand	Y	Y	Y	Y	Y	Y
DPD periodic message option	N	N	Y	Y	Y	Y
IPSec prefragmentation (Look-Ahead Fragmentation, or LAF)	Y	Y	Y	Y	Y	Y
Reverse Route Injection (RRI)	Y	Y	Y	Y	Y	Y
Reverse route with optional parameters	N	N	N	N	N	N
Adjustable IPSec anti-replay window size	N	Y	Y	Y	Y	Y
IPSec preferred peer	Y	Y	Y	Y	Y	Y
Per-crypto map (and global) IPSec security association (SA) idle timers	Y	Y	Y	Y	Y	Y
Distinguished name-based crypto maps	Y	Y	Y	Y	Y	Y
Sequenced access control lists (ACLs) (crypto ACLs)	Y	Y	Y	Y	Y	Y

Table 25-1 IPSec Feature Support By Release in All VPN Modes for SPA-IPSEC-2G (continued)

Feature Name	**Cisco IOS Software Release 12.2**					**Cisco IOS Release 15S**
	SXE	**SXF**	**SRA**	**SRB, SRC,** SRD,SRE	**SXH**[1]	15.0 (1)S and later
Deny policy configuration enhancements (drop, jump, clear)	Y	Y	Y	Y	Y	Y
Disable volume lifetime per interface	N	N	N	N	N	N
IPSec VPN SPA quality of service (QoS) queueing	Y	Y	Y	Y	Y	Y
Multiple RSA key pair support	N	N	Y	Y	Y	Y
Protected private key storage	N	N	Y	Y	Y	Y
Trustpoint CLI	N	N	Y	Y	Y	Y
Query mode per trustpoint	N	N	N	N	N	N
Local certificate storage location	N	N	Y	Y	Y	Y
Direct HTTP enroll with CA servers	Y	Y	Y	Y	Y	Y
Manual certificate enrollment (TFTP and cut-and-paste)	N	N	Y	Y	Y	Y
Certificate autoenrollment	N	N	Y	Y	Y	Y
Key rollover for Certificate Authority (CA) renewal	N	N	N	N	N	N
Public-key infrastructure (PKI) query multiple servers	N	N	N	N	N	N
Online Certificate Status Protocol (OCSP)	N	N	N	N	N	N
Optional OCSP nonces	N	N	N	N	N	N
Certificate security attribute-based access control	N	N	N	N	N	N
PKI AAA authorization using entire subject name	N	N	N	N	N	N
PKI local authentication using subject name	N	N	Y	Y	Y	Y
Source interface selection for outgoing traffic with certificate authority	N	N	N	N	N	N
Persistent self-signed certificates as Cisco IOS CA server	N	N	N	N	N	N
Certificate chain verification	N	N	N	N	N	N
Multi-tier certificate support	Y	Y	Y	Y	Y	Y
Easy VPN Server enhanced features	N	N	N	N	N	N

Table 25-1 IPSec Feature Support By Release in All VPN Modes for SPA-IPSEC-2G (continued)

Feature Name	**Cisco IOS Software Release 12.2**					**Cisco IOS Release 15S**
	SXE	**SXF**	**SRA**	**SRB, SRC,** SRD,SRE	**SXH**[1]	15.0 (1)S and later
Easy VPN Server basic features	Y	Y	Y	Y	Y	Y
Interoperate with Easy VPN Remote using preshared key	Y	Y	Y	Y	Y	Y
Interoperate with Easy VPN Remote using RSA signature	N	N	Y	Y	Y	Y
Stateless failover using the Hot Standby Router Protocol (HSRP)	Y	Y	Y	Y	Y	Y
Chassis-to-chassis stateful failover using HSRP and SSP in site-to-site IPSec using preshared keys with crypto maps	Y	Y	N	N	N	N
Chassis-to-chassis failover (IPSec stateful failover) with DMVPN, GRE/TP, VTI, Easy VPN, or PKI	N	N	N	N	N	N
Blade-to-Blade stateful failover	Y	Y	Y	Y	Y	Y
IPSec VPN Monitoring (IPSec Flow MIB)	Y	Y	Y	Y	Y	Y
IPSec VPN Accounting (start / stop / interim records)	Y	Y	Y	Y	Y	Y
Crypto Conditional Debug support	N	Y	Y	Y	Y	Y
show crypto engine accelerator statistic command	N	N	Y	Y	Y	Y
Other **show crypto engine** commands	N	N	N	N	N	N
clear crypto engine accelerator counter command	N	N	Y	Y	Y	Y
Crypto commands applied to a loopback interface	N	N	N	N	N	N
Policy Based Routing (PBR) on tunnel interface or interface VLAN	N	N	N	N	N	N
ACL on tunnel interface	N	N	N	N	N	N
MQC QoS on tunnel interface (service policy)	N	N	N	N	N	N
mls qos command on all tunnel interfaces: IPSec, GRE, mGRE	N	N	N	N	N	N
QoS pre-classify CLI	N	N	N	N	N	N
NAT on crypto VLAN or crypto protected tunnel interface	N	N	N	N	N	N

Table 25-1 IPSec Feature Support By Release in All VPN Modes for SPA-IPSEC-2G (continued)

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Release 15S
	SXE	**SXF**	**SRA**	**SRB, SRC,** SRD,SRE	**SXH**[1]	15.0 (1)S and later
16 K tunnels (IKE and IPSec tunnels)	N	N	Y	Y	Y	Y
Switching between VRF and crypto-connect modes requires reboot	Y	Y	Y	Y	Y	Y
GRE keepalives on tunnel protection (TP) tunnels	N	N	N	N	N	N
GRE keepalives on mGRE/DMVPN tunnels	N	N	N	N	N	N
IPSec Network Address Translation Transparency (NAT-T) (transport mode, ESP only)	Y	Y	Y	Y	Y	Y
Dynamic Multipoint VPN Phase 2 (DMVPN) (mGRE; TP & NHRP)	Y	Y	Y	Y	Y	Y
DMVPN Phase 3	N	N	N	N	N	N
DMVPN hub router behind a NAT gateway—tunnel mode	N	N	N	N	N	N
DMVPN hub router behind a NAT gateway—transport mode (not spoke-to-spoke)	N	N	N	N	Y	N
DMVPN spoke router behind a NAT gateway—tunnel mode	N	N	N	N	N	N
DMVPN spoke router behind a NAT gateway—transport mode (not spoke-to-spoke)	Y	Y	Y	Y	Y	Y
Multicast transit traffic over DMVPN tunnels	N	N	N	N	N	N
Non-IP traffic over TP (DMVPN, point-to-point GRE, sVTI) tunnels	N	N	N	N	N	N
Support for the VPNSM	Y	Y	N	N	N	N
All serial PPP interfaces with crypto-connect mode must have **ip unnumber null 0** command	N	N	N	Y	Y	Y
Manual key	N	Y	N	N	N	N
Tunnel Endpoint Discovery	Y	Y	N	N	N	N
Transport adjacency and nested tunnels	N	N	N	N	N	N
Transit IPSec packets	N	Y	N	N	Y	N

Table 25-1 IPSec Feature Support By Release in All VPN Modes for SPA-IPSEC-2G (continued)

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Release 15S
	SXE	SXF	SRA	SRB, SRC, SRD,SRE	SXH[1]	15.0 (1)S and later
IPSec VPN SPA supported with virtual switching system (VSS)	N	N	N	N	N	N
IP header options through IPSec tunnels	N	N	N	N	N	N
Invalid SPI recovery	N	N	Y	Y	Y	Y
IPSec compression	N	N	N	N	N	N
Multilink or dialer interfaces	N	N	N	N	N	N
Group Encrypted Transport VPN (GETVPN)	N	N	N	N	N	N
IPSec Passive Mode	N	N	N	N	N	N

[1] The SXH software release is for the Catalyst 6500 series switch. This release does not apply to the Cisco 7600 series router.

Table 25-2 lists the supported and unsupported IPSec features common to all VPN modes for WS-IPSEC-3 IPSEC VSPA.

Table 25-2 IPSec Feature Support in All VPN Modes for WS-IPSEC-3 SPA

Feature Name	Cisco IOS Release 15.1(3)S1
IPSec tunnels using software crypto	N
Enhanced GRE takeover (if the supervisor engine cannot process)	Y
Multicast over GRE	Y
Multicast over multipoint GRE (mGRE) / DMVPN	N
Multicast Scalability Enhancement (single SPA mode)	Y
Advanced Encryption Standard (AES)	Y
Internet Security Association and Key Management Protocol (ISAKMP) keyring	Y
SafeNet Client support	Y
Peer filtering (SafeNet Client support)	N
Certificate to ISAKMP profile mapping	Y
Encrypted preshared key	Y
IKE Aggressive Mode Initiation	N
Call Admission Control (CAC) for IKE	Y
Dead Peer Detection (DPD) on-demand	Y
DPD periodic message option	Y

Table 25-2 IPSec Feature Support in All VPN Modes for WS-IPSEC-3 (continued) SPA

Feature Name	Cisco IOS Release 15.1(3)S1
IPSec prefragmentation (Look-Ahead Fragmentation, or LAF)	Y
Reverse Route Injection (RRI)	Y
Reverse route with optional parameters	N
Adjustable IPSec anti-replay window size	Y
IPSec preferred peer	Y
Per-crypto map (and global) IPSec security association (SA) idle timers	Y
Distinguished name-based crypto maps	Y
Sequenced access control lists (ACLs) or crypto ACLs	Y
Deny policy configuration enhancements (drop, jump, clear)	Y
Disable volume lifetime per interface	N
IPSec VPN SPA quality of service (QoS) queueing	Y
Multiple RSA key pair support	Y
Protected private key storage	Y
Trustpoint CLI	Y
Query mode per trustpoint	N
Local certificate storage location	Y
Direct HTTP enroll with CA servers	Y
Manual certificate enrollment (TFTP and cut-and-paste)	Y
Certificate autoenrollment	Y
Key rollover for Certificate Authority (CA) renewal	N
Public-key infrastructure (PKI) query multiple servers	N
Online Certificate Status Protocol (OCSP)	N
Optional OCSP nonces	N
Certificate security attribute-based access control	N
PKI AAA authorization using entire subject name	N
PKI local authentication using subject name	Y
Source interface selection for outgoing traffic with certificate authority	N
Persistent self-signed certificates as Cisco IOS CA server	N
Certificate chain verification	N
Multi-tier certificate support	Y
Easy VPN Server enhanced features	N
Easy VPN Server basic features	Y

Table 25-2 IPSec Feature Support in All VPN Modes for WS-IPSEC-3 (continued) SPA

Feature Name	Cisco IOS Release 15.1(3)S1
Interoperate with Easy VPN Remote using preshared key	Y
Interoperate with Easy VPN Remote using RSA signature	Y
Stateless failover using the Hot Standby Router Protocol (HSRP)	Y
Chassis-to-chassis stateful failover using HSRP and SSP in site-to-site IPSec using preshared keys with crypto maps	N
Chassis-to-chassis failover (IPSec stateful failover) with DMVPN, GRE/TP, VTI, Easy VPN, or PKI	N
Blade-to-Blade stateful failover	Y
IPSec VPN Monitoring (IPSec Flow MIB)	Y
IPSec VPN Accounting (start / stop / interim records)	Y
Crypto Conditional Debug support	Y
show crypto engine accelerator statistic command	Y
clear crypto engine accelerator counter command	Y
Crypto commands applied to a loopback interface	N
Policy Based Routing (PBR) on tunnel interface or interface VLAN	N
ACL on tunnel interface	N
MQC QoS on tunnel interface (service policy)	N
mls qos command on all tunnel interfaces: IPSec, GRE, mGRE	N
QoS pre-classify CLI	N
NAT on crypto VLAN or crypto protected tunnel interface	N
16000 tunnels (IKE and IPSec tunnels)	Y
Switching between VRF and crypto-connect modes requires reboot	Y
GRE keepalives on tunnel protection (TP) tunnels	N
GRE keepalives on mGRE/DMVPN tunnels	N
IPSec Network Address Translation Transparency (NAT-T) (transport mode, ESP only)	Y
DMVPN Phase 2 (mGRE; TP & NHRP)	Y
DMVPN Phase 3	N
DMVPN hub router behind a NAT gateway—tunnel mode	N
DMVPN hub router behind a NAT gateway—transport mode (not spoke-to-spoke)	N

Table 25-2 IPSec Feature Support in All VPN Modes for WS-IPSEC-3 (continued) SPA

Feature Name	Cisco IOS Release 15.1(3)S1
DMVPN spoke router behind a NAT gateway—tunnel mode	N
DMVPN spoke router behind a NAT gateway—transport mode (not spoke-to-spoke)	Y
Multicast transit traffic over DMVPN tunnels	N
Non-IP traffic over TP (DMVPN, point-to-point GRE, sVTI) tunnels	N
Support for the VPNSM	N
All serial PPP interfaces with crypto-connect mode must have **ip unnumber null 0** command	Y
Manual key	N
Tunnel Endpoint Discovery	N
Transport adjacency and nested tunnels	N
Transit IPSec packets	N
IPSec VPN SPA supported with virtual switching system (VSS)	N
IP header options through IPSec tunnels	N
Invalid Security Parameter Index (SPI) recovery	Y
IPSec compression	N
Multilink or dialer interfaces	N
Group Encrypted Transport VPN (GETVPN)	N
IPSec Passive Mode	N

IPSec Features in Crypto-Connect Mode

Table 25-3 lists the supported and unsupported IPSec features in crypto-connect mode for SPA-IPSEC-2G.

Table 25-3 IPSec Feature Support By Release in Crypto-Connect Mode for SPA-IPSEC-2G

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Software Release 15S
	SXE	SXF	SRA	SRB, SRC, SRD,SRE	SXH[1]	15.0(1)S and later
Point-to-point GRE with tunnel protection and VTI	N	N	N	N	N	N
Path MTU discovery (PMTUD)	N	N	Y	Y	Y	Y
PMTUD with NAT-T	N	N	N	N	N	N
IPSec static virtual tunnel interface (sVTI)	N	N	N	N	N	N
The use of VRFs in conjunction with crypto features	N	N	N	N	N	N
IPX and Appletalk over point-to-point GRE	Y	Y	Y	Y	Y	Y
ip tcp adjust-mss command in GRE when taken over	N	N	N	N	N	N

[1] The SXH software release is for the Catalyst 6500 series switch. This release does not apply to the Cisco 7600 series router.

Table 25-3 lists the supported and unsupported IPSec features in crypto-connect mode for the WS-IPSEC-3 SPA.

Table 25-4 Supported and Unsupported IPSec Features in Crypto-Connect Mode for WS-IPSEC-3 SPA

Feature Name	Cisco IOS Software Release 15.1(3)S1
Point-to-point GRE with tunnel protection	N
Path MTU discovery (PMTUD)	N
PMTUD with NAT-T	N
IPSec static virtual tunnel interface (sVTI)	N
The use of VRFs in conjunction with crypto features	N
IPX and Appletalk over point-to-point GRE	Y
ip tcp adjust-mss command in GRE when taken over	N

IPSec Features in VRF Mode

Table 25-5 lists the supported and unsupported IPSec features in VRF mode for SPA-IPSEC-2G IPSEC VPN SPA.

Table 25-5 IPSec Feature Support in VRF Mode for SPA-IPSEC-2G IPSEC VPN SPA

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Software Release 15S
	SXE	SXF	SRA	SRB, SRC, SRD,SRE	SXH[1]	15.0(1)S and later
Global VRF	Y	Y	Y	Y	Y	Y
Front-door VRF (FVRF)	N	N	Y	Y	Y	Y
FVRF on an mGRE tunnel configured on a DMVPN hub	N	N	Y	Y	Y	Y
FVRF on an mGRE tunnel configured on a DMVPN spoke	N	N	N	N	N	N
Overlapping IP address space in VRFs	Y	Y	Y	Y	Y	Y
Secondary IP addresses on interfaces	N	N	N	N	N	N
MPLS over GRE/IPSec (tag switching on tunnel interfaces)	N	N	N	N	N	N
PE-PE encryption (IPSec only) over MPLS	N	N	N	N	N	N
PE-PE encryption (tunnel protection) over MPLS	N	N	N	N	N	N
MPLS PE-CE encryption (Tag2IP) with GRE/TP	N	N	N	Y	Y	Y
MPLS PE-CE encryption (Tag2IP) with sVTI	N	N	N	N	N	N
MPLS PE-CE encryption (Tag2IP) with crypto map	N	N	N	N	N	N
Crypto maps in VRF-lite	Y	Y	Y	Y	Y	Y
Per-VRF AAA with RADIUS	N	N	N	Y	Y	Y
Per-VRF AAA with TACACS	N	N	N	Y	N	Y
IPSec static virtual tunnel interface (sVTI)	N	N	Y	Y	Y	Y
Multicast over sVTI	N	N	N	N	N	N
ip tcp adjust-mss command on sVTI or GRE	N	N	N	N	N	N
Ingress and egress features (ACL, QOS) on sVTI, GRE/TP, and mGRE tunnel	N	N	N	N	N	N

Table 25-5 *IPSec Feature Support in VRF Mode (continued)for SPA-IPSEC-2G IPSEC VPN SPA*

Feature Name	Cisco IOS Software Release 12.2					Cisco IOS Software Release 15S
	SXE	SXF	SRA	SRB, SRC, SRD,SRE	SXH[1]	15.0(1)S and later
Ingress features (ACL, PBR, inbound service policy) on the outside interface	N	N	N	N	N	N
Outbound service policy on the outside interface	Y	Y	Y	Y	Y	Y
TP support in the global context	N	N	Y	Y	Y	Y
IPSec SA using crypto map created in transport mode	N	N	N	N	N	N
Path MTU discovery (PMTUD)	N	N	N	N	N	N
Non-IP version 4 traffic over TP tunnels	N	N	N	N	N	N
IPv6 IPSec sVTI IPv6-in-IPv6	N	N	N	N	N	N

[1] The SXH software release is for the Catalyst 6500 series switch. This release does not apply to the Cisco 7600 series router.

Table 25-6 lists the supported and unsupported IPSec features in VRF mode for WS-IPSEC-3 IPSEC VSPA.

Table 25-6 *Supported and Unsupported IPSec Features in VRF Mode for WS-IPSEC-3 IPSEC VSPA*

Table 25-7

Feature Name	Cisco IOS Software Release 15.1(3)S1
Global VRF	Y
Front-door VRF (FVRF)	Y
FVRF on an mGRE tunnel configured on a DMVPN hub	Y
FVRF on an mGRE tunnel configured on a DMVPN spoke	N
Overlapping IP address space in VRFs	Y
Secondary IP addresses on interfaces	N
MPLS over GRE/IPSec (tag switching on tunnel interfaces)	N
PE-PE encryption (IPSec only) over MPLS	N
PE-PE encryption (tunnel protection) over MPLS	N
MPLS PE-CE encryption (Tag2IP) with GRE/TP	Y

Table 25-7

Feature Name	Cisco IOS Software Release 15.1(3)S1
MPLS PE-CE encryption (Tag2IP) with sVTI	N
MPLS PE-CE encryption (Tag2IP) with crypto map	N
Crypto maps in VRF-lite	Y
Per-VRF AAA with RADIUS	Y
Per-VRF AAA with Terminal Access Controller Access-Control System (TACACS)	Y
IPSec static virtual tunnel interface (sVTI)	Y
Multicast over sVTI	N
ip tcp adjust-mss command on sVTI or GRE	N
Ingress and egress features (ACL, QOS) on sVTI, GRE/TP, and mGRE tunnel	N
Ingress features (ACL, PBR, inbound service policy) on the outside interface	N
Outbound service policy on the outside interface	Y
TP support in the global context	Y
IPSec SA using crypto map created in transport mode	N
Path MTU discovery (PMTUD)	N
Non-IP version 4 traffic over TP tunnels	N
IPv6 IPSec sVTI IPv6-in-IPv6	N

Interoperability for SPA-IPSEC-2G IPSEC VPN SPA

Supervisor Engine support varies based on the release. Table 25-8 lists the supported Supervisor Engines for each release for the SPA-IPSEC-2G IPSec VPN SPA.

Table 25-8 Supervisor Engine Support for the SPA-IPSEC-2G IPSec VPN SPA by Release

Release	Supervisor Supported
Cisco IOS Release 12.2(33)SRE	Supervisor Engine RSP720-10GE Supervisor Engine RSP720-1GE Supervisor Engine 720 Supervisor Engine 32
Cisco IOS Release 12.2(33)SRC	Supervisor Engine RSP720-1GE Supervisor Engine 720 Supervisor Engine 32

Table 25-8 Supervisor Engine Support for the SPA-IPSEC-2G IPSec VPN SPA by Release

Release	Supervisor Supported
Cisco IOS Release 12.2(33)SRA	Supervisor Engine 720 Supervisor Engine 32
Cisco IOS Release 12.2(18)SXF2	Supervisor Engine 720 Supervisor Engine 32 Supervisor Engine 2
Cisco IOS Release 12.2(18)SXE5	Supervisor Engine 720
Cisco IOS Release 12.2(18)SXE2	Supervisor Engine 720

Line card module support varies based on the release.

The IPSec VPN SPA supports the following interoperability features:

- You may have an IPSec VPN SPA in the same chassis with the following service modules:
  - Firewall Services Module (WS-SVC-FWM-1-K9)
  - Network Analysis Module 2 (WS-SVC-NAM-2)

Table 25-9 lists the known supported line card modules for each release. Note the following guidelines when using this table:

- An “X” in the Qualified column indicates the module was tested; an “X” in the Supported column indicates that the module is supported.
- If the module has a footnote beside the “X” in the Supported column, although the module is supported, some restrictions apply. See the footnote below the table for details of the restriction.
- If the module has an “X” in the Supported column but not in the Qualified column, although the module was not specifically tested, it is supported.

Any line card modules not specifically listed in the table are not supported by TAC/BU.

Table 25-9 Line Card Module Support for the SPA-IPSEC-2G IPSec VPN SPA by Release

Line Card Module	Cisco IOS Release 12.2(18)SX		Cisco IOS Release 12.2(33)SR	
	Qualified	Supported	Qualified	Supported
7600-SIP-200 With the following SPAs: SPA-2XOC3-ATM= SPA-2XOC3-POS= SPA-2XT3/E3	X	X	X	X
7600-SIP-400 With the following SPAs: SPA-1XOC12-ATM= SPA-2X0C3-ATM= SPA-2X1GE		X[1]	X[2]	X
7600-SIP-600 With the following SPAs: SPA-1X10GE SPA-10X1GE			X[3]	X

Table 25-9 Line Card Module Support for the SPA-IPSEC-2G IPSec VPN SPA by Release (continued)

Line Card Module	Cisco IOS Release 12.2(18)SX		Cisco IOS Release 12.2(33)SR	
7600-SSC-400	X	X	X	X
OSM-2OC48/1DPT-SI		X		X
OSM-2OC48/1DPT-SL		X		X
OSM-2OC48/1DPT-SS	X	X		X
OSM-8OC3-POS-MM	X	X	X	X
OSM-8OC3-POS-SI		X		X
OSM-8OC3-POS-SI+		X		X
OSM-8OC3-POS-SL		X		X
OSM-16OC3-POS-MM+	X	X	X	X
OSM-16OC3-POS-SI		X		X
OSM-16OC3-POS-SI+		X		X
OSM-16OC3-POS-SL		X		X
OSM-2+4GE-WAN+	X	X		X
WS-6182-2PA	X	X	X	X
WS-6582-2PA	X	X	X	X
WS-6802-2PA With the following PAs: PA-A3-OC3MM PA-A3-T3 PA-MC-T3	X	X		X
WS-SVC-FWM-1	X	X		X
WS-SVC-IDSM2	X	X		
WS-SVC-IDSUPG	X	X		
WS-SVC-NAM2	X	X		
WS-SVC-WEBVPN-K9	X	X		X
WS-X6148-GE-TX	X	X	X	X
WS-X6408A-GBIC	X	X		X
WS-X6416-GBIC	X	X		X
WS-X6416-GE-MT		X		X
WS-X6502-10GE	X	X	X	X
WS-X6516-GBIC	X	X	X	X
WS-X6516-GE-TX	X	X	X	X
WS-X6516A-GBIC	X	X	X	X
WS-X6548-GE-TX	X	X	X	X
WS-X6548V-GE-TX		X		X
WS-X6548-RJ-21		X		X
WS-X6548-RJ-45	X	X	X	X

Table 25-9 Line Card Module Support for the SPA-IPSEC-2G IPSec VPN SPA by Release (continued)

Line Card Module	Cisco IOS Release 12.2(18)SX		Cisco IOS Release 12.2(33)SR	
WS-X6704-10GE	X	X	X	X
WS-X6724-SFP	X	X	X	X
WS-X6748-GE-TX	X	X	X	X
WS-X6748-SFP	X	X	X	X

[1] Cisco IOS Release 12.2(18)SXF2: Switch port configurations are not supported when a Cisco 7600 SIP-400 is present in the chassis.

[2] Cisco IOS Release 12.2(33)SRA: Switch port configurations are not supported when a Cisco 7600 SIP-400 is present in the chassis.

[3] Cisco IOS Release 12.2(33)SRA: MPLS tunnel recirculation must be enabled when a Cisco 7600 SIP-600 is installed and VRF is to be enabled. That is, you must add the **mls mpls tunnel-recir** command before entering the **crypto engine mode vrf** command if a Cisco 7600 SIP-600 is present in the chassis.

Restrictions

Note For other SSC-specific features and restrictions see also Chapter 4, "Overview of the SIPs and SSC"in this guide.

The IPSec VPN SPAs are subject to the following restrictions:

Restrictions for SPA-IPSEC-2G IPSEC VPN SPA

- The SPA-IPSEC-2G IPSec VPN SPA requires Cisco IOS Release 12.2(18)SXE2 or later releases.
- The SPA-IPSEC-2G IPSec VPN SPA is supported only on the Cisco 7600 SSC-400.
- The Cisco 7600 SSC-400 is not Route Processor Redundancy Plus (RPR+) or Stateful Switchover (SSO) aware. As a result, the Cisco 7600 SSC-400 will reset if RPR+ or SSO is configured.
- The Unicast Reverse Path Forwarding (uRPF) uses ACL to redirect packets to the software. The uRPF check with crypto ACL is not supported in the hardware in the CCA mode.
- As of Cisco IOS Release 12.2(33)SRA, the SPA-IPSEC-2G IPSec VPN SPA is only supported on a Cisco 7600 series router using a Supervisor Engine 720 (MSFC3 and PFC3) with a minimum of 512 MB memory or a Supervisor Engine 32. For a list of the Supervisor Engine support for each release, see Table 25-8 on page 25-20.

  Note The IPSec VPN SPA MSFC DRAM requirements are as follows:

  – Up to 8,000 tunnels with 512-MB DRAM
  – Up to 16,000 tunnels with 1-GB DRAM

  These numbers are chosen to leave some memory available for routing protocols and other applications. However, your particular use of the MSFC may demand more memory than the quantities that are listed above. In an extreme case, you could have one tunnel but still require 512-MB DRAM for other protocols and applications running on the MSFC.

- Only the following Cisco 7600 series routers are supported:
  - 7603 router (CISCO7603)

- 7604 router (CISCO7604)
- 7606 router (CISCO7606)
- 7609 router (CISCO7609)
- 7609 router (OSR-7609)
- 7613 router (CISCO7613)

Note Supervisor Engine RSP720-10GE is supported only on 7606 S-Chasis (CISCO7606-S) and is not supported on (CISCO7606).

- A maximum of 10 IPSec VPN SPAs per chassis are supported.
- As of Cisco IOS Release 12.2(33)SRA, a maximum number of 2000 IPSec tunnels is supported when PKI is configured with the SPA-IPSEC-2G IPSec VPN SPA.
- TCP ADJUST-MSS is NOT supported on VTI tunnel in Cisco 7600 Release 12.2(33) SRB.
- GRE keepalives are not supported if **crypto engine gre vpnblade** is configured.

Note In Cisco IOS Release 12.2(18)SXF2 and later releases, the **crypto engine subslot** command used in previous releases has been replaced with the **crypto engine slot** command (of the form **crypto engine slot** *slot/subslot* {**inside** | **outside**}). The **crypto engine subslot** command is no longer supported.

When upgrading, ensure that this command has been modified in your start-up configuration to avoid extended maintenance time.

- Applying the **crypto engine slot outside** command on Port-Channel interface is not supported.
- Owing to it having reached EoS in its lifecycle, no active release supports SPA-IPSEC-2G IPSec SPA.
- As SPA-IPSEC-2G IPSec SPA has reached EoS, migrate to WS-IPSEC-3 IPSec VSPA. For more information, see http://www.cisco.com/en/US/partner/prod/collateral/modules/ps6267/end_of_life_c51-583910.html

Restrictions for WS-IPSEC-3 IPSEC VSPA

Following restrictions apply for WS-IPSEC-3 IPSec VSPA with Cisco 7600:

- The WS-IPSEC-3 IPSec VSPA is supported only on the Cisco 7600 SSC-600 line card.
- The WS-IPSEC-3 IPSec VSPA is available on Cisco IOS Release 15.1(3)S1 or later releases.
- The WS-IPSEC-3 IPSec VSPA is supported on SUP32, SUP720, RSP720-1GE and RSP720-10GE supervisors on the Cisco 7600 platform.
- Any combination of encapsulating security payload (ESP) and authentic header (AH) transform set is not supported by WS-IPSEC-3 IPSec VSPA. You should avoid this combination while configuring transform set on WS-IPSEC-3 IPSec VSPA.
- You cannot combine a SPA-IPSEC-2G IPSec VPN SPA and a WS-IPSEC-3 IPSec VSPA in a blade failover group (BFG).

- When you are using 2-IPSEC-3G SPAs in one 7600 chassis, we cannot scale single VLAN capable of more than 4 Gbps as mapping needs to be done separately. We have to send two traffic stream for different VLANs. Each VLAN100 and VLAN 101 will receive 5Gbps and it is not possible to load balance single VLAN flow across the TWO IPSEC-3G SPA.
- Adding a second IPSEC-3G SPA will not increase the throughput rate 16 Gbps full duplex. We have to configure statically with two different VLANs (VLAN100, VLAN101) for two VRFs (IVRF, SVRF). So each VRF is capable of 4Gbps since we can increase the IPSEC-3G throughput rate 16 Gbps bidirectional (full duplex).

Note Effective from Cisco IOS release 15.1(3)S3 if you configure the crypto engine **hw-FIPS-mode** command on a Cisco 7600 router and the FIPS self test fails for any of the WS-IPSEC-3 IPsec VSPA, the router reloads continuously till the router passes the FIPS self test.

Support for WS-IPSEC-3 IPSec VSPA on Cisco Routers

The following Cisco router series support WS-IPSEC-3 IPSec VSPA:

- 7603 router (CISCO7603)
- 7604 router (CISCO7604)
- 7606 router (CISCO7606)
- 7609 router (CISCO7609)
- 7613 router (CISCO7613)

Supported MIBs

The following MIBs are supported as of Cisco IOS Release 12.2(18)SXE2 for the Cisco 7600 SSC-400 and the SPA-IPSEC-2G IPSec VPN SPA on a Cisco 7600 series router:

- CISCO-IPSEC-FLOW-MONITOR-MIB

Note Gigabit Ethernet port SNMP statistics (for example, ifHCOutOctets and ifHCInOctets) are not provided for the internal IPSec VPN SPA trunk ports because these ports are not externally operational ports and are used only for configuration.

For more information about MIB support on a Cisco 7600 series router, refer to the *Cisco 7600 Series Router MIB Specifications Guide*, at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you.

IPSec VPN SPA Hardware Configuration Guidelines

The configuration guidelines for IPSec VPN SPA hardware are as follows:

- For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* and *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* publications.
- Some CLI commands require you to specify the inside and outside ports of the IPsec VPN Module in the format *slot/subslot/port*. Although the IPsec VPN Module ports are not actual Gigabit Ethernet ports, and do not share all properties of external Gigabit Ethernet interfaces, they can be addressed for configuration as Gigabit Ethernet trunk ports, using port numbers as follows:
  - Port 1—Inside port, attached to interface VLAN
  - Port 2—Outside port, attached to port VLAN

  For example, to configure the outside port of a IPsec VPN Module in the first subslot (subslot 0) of an Cisco 7600 SSC-400 in slot 6 of a Cisco 7600 series router, enter the following command:

  ```
  Router(config)# interface GigabitEthernet6/0/2
  ```
- The **show crypto engine configuration** command does not show the IPSec VPN SPA subslot number when there is no crypto connection even if the adapter is installed in the chassis.
- When you remove an IPSec VPN SPA that has some ports participating in crypto connections, the crypto configuration remains intact. When you reinsert the same type of IPSec VPN SPA into the same slot, the crypto connections will be reestablished. To move the IPSec VPN SPA to a different slot, you must first manually remove the crypto connections before removing the IPSec VPN SPA. You can enter the **no crypto connect vlan** command from any interface when the associated physical port is removed.
- When you reboot an IPSec VPN SPA that has crypto connections, the existing crypto configuration remains intact. The crypto connections will be reestablished after the IPSec VPN SPA reboots. When a crypto connection exists but the associated interface VLAN is missing from the IPSec VPN SPA inside port, the crypto connection is removed after the IPSec VPN SPA reboots.
- When you remove a port VLAN or an interface VLAN with the **no interface vlan** command, the associated crypto connection is also removed.

Displaying the SPA Hardware Type

There are several commands on the Cisco 7600 series router that provide IPSec VPN SPA hardware information.

- To verify the SPA hardware type that is installed in your router, use the **show module** command.
- To display hardware information for the IPSec VPN SPA, use the **show crypto eli** command.

For more information about these commands, see the *Cisco 7600 Series Router Command Reference, 12.2SR*.

Example of the show module Command

The following example shows output from the **show module** command on a Cisco 7600 series router with an IPSec VPN SPA installed in subslot 0 of a Cisco 7600 SSC-400 that is installed in slot 4:

```
Router# show module 4
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  4    0  2-subslot Services SPA Carrier-400     7600-SSC-400       JAB1104013N

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  4  001a.a1aa.95f0 to 001a.a1aa.962f   2.0   12.2(33)SXH  12.2(33)SXH  Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
 4/0 2 Gbps IPSec SPA            SPA-IPSEC-2G       JAB1048075L  1.0    Ok

Mod  Online Diag Status
---- -------------------
  4  Pass
 4/0 Pass

The following is a sample output from the show module command on a Cisco 7600 series
router with a WS-IPSEC-3 IPSec VSPA installed in subslot 1 of a Cisco 7600 SSC-600 that is
installed in slot 2:
Router# show module 2
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  2    0  2-subslot Services SPA Carrier-600     WS-SSC-600         SAL144705A5

Mod MAC addresses                       Hw    Fw            Sw           Status
--- ---------------------------------- ----- ------------- ------------ -------
  2  e05f.b9a1.5b50 to e05f.b9a1.5b57  1.0   15.1(NTLYIND_ 15.1(NTLYIND Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
 2/1 IPSec Accelerator 3         WS-IPSEC-3         SAL150353Y7  1.1    Ok

Mod  Online Diag Status
---- -------------------
  2  Pass
 2/1 Pass
```

Example of the show crypto eli Command

The following example shows output from the **show crypto eli** command on a Cisco 7600 series router with IPSec VPN SPAs installed in subslots 0 and 1 of a Cisco 7600 SSC-400 that is installed in slot 3. The output displays how many IKE-SAs and IPSec sessions are active and how many Diffie-Hellman keys are in use for each IPSec VPN SPA.

```
Router# show crypto eli

Hardware Encryption : ACTIVE
Number of hardware crypto engines = 2

CryptoEngine SPA-IPSEC-2G[3/0] details: state = Active
Capability      :
    IPSEC: DES, 3DES, AES, RSA
```

```
IKE-Session   :     0 active, 16383 max, 0 failed
DH            :     0 active,  9999 max, 0 failed
IPSec-Session :     0 active, 65534 max, 0 failed

CryptoEngine SPA-IPSEC-2G[3/1] details: state = Active
Capability      :
    IPSEC: DES, 3DES, AES, RSA

IKE-Session   :     1 active, 16383 max, 0 failed
DH            :     0 active,  9999 max, 0 failed
IPSec-Session :     2 active, 65534 max, 0 failed

Router#
```

The following is a sample output from the **show crypto eli** command on a Cisco 7600 series router with IPSec VSPA installed in subslot 1 of a Cisco 7600-SSC-600 that is installed in slot 2. The output displays how many IKE-SAs and IPSec sessions are active and how many Diffie-Hellman keys are in use for each IPSec VSPA.

```
Router# show crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1

CryptoEngine WS-IPSEC-3[2/1] details: state = Active
Capability    : DES, 3DES, AES, RSA

 IKE-Session   :     0 active, 16383 max, 0 failed
 DH            :     0 active,  9999 max, 0 failed
 IPSec-Session :     0 active, 65534 max, 0 failed
```