CHAPTER 2

Overview of the IPsec Features

This chapter provides an overview of the IPsec features of the VSPA.

This chapter includes the following sections:

Overview of Basic IPsec and IKE Configuration Concepts

This section reviews some basic IPsec and IKE concepts that are used throughout the configuration of the VSPA, 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 or switches. 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, or crypto ACLs, 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.

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 switch 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 enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is enabled by default.

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.)

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 7-2.

Configuring VPNs with the VSPA

To configure a VPN using the VSPA, 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 VSPA 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 VSPA using crypto-connect mode, you attach crypto maps to VLANs (using interface VLANs); when you configure VPNs on switches running Cisco IOS software, you configure individual interfaces.

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

Crypto-connect mode VPN configuration is described in Chapter 3, "Configuring VPNs in Crypto-Connect Mode."

VRF Mode

The VRF-aware IPsec feature, known as VRF mode, 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 VSPA 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 4, "Configuring VPNs in VRF Mode."

Overview of the VSPA Features

The VSPA provides hardware acceleration for policy enforcement and bulk encryption and forwarding. The following features are supported:

- IPv4
  - crypto maps
  - static VTI
  - GRE/DMVPN
  - 16K tunnels
- IPv6
  - static VTI
  - IPv6-in-IPv6 (6in6) tunnels
- IKE acceleration
- AES/DES/3-DES encryption algorithms and SHA-1/MD5 hashing algorithms
- Packet classification in IPv4

IPsec Feature Support

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

- IPsec Features Common To All VPN Modes, page 2-5
- IPsec Features in Crypto-Connect Mode, page 2-8
- IPsec Features in VRF Mode, page 2-9

Note This configuration guide describes VSPA features and applications that have been tested and are supported. Features and applications that do not explicitly appear in the Feature 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 2-1 displays supported and unsupported IPsec features common to all VPN modes.

Table 2-1 IPsec Feature Support By Release in All VPN Modes

Feature Name	Software Release 12.2
	SXI
IPsec tunnels using software-based cryptography	N
Enhanced generic router encapsulation (GRE) takeover (if supervisor engine cannot process)	Y
Multicast over GRE	Y
Multicast over multipoint GRE (mGRE) / DMVPN	N
Multicast Scalability Enhancement (single SPA mode)	N
Advanced Encryption Standard (AES)	Y
ISAKMP keyring	Y
SafeNet Client support	N
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
IPsec prefragmentation (Look-Ahead Fragmentation, or LAF)	Y
Reverse Route Injection (RRI)	Y
Reverse route with optional parameters	N

Table 2-1 IPsec Feature Support By Release in All VPN Modes (continued)

Feature Name	Software Release 12.2
	SXI
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) (crypto ACLs)	Y
Deny policy configuration enhancements (drop, clear)	Y
Disable volume lifetime per interface	Y
VSPA quality of service (QoS) queueing	Y
Multiple RSA key pair support	Y
Protected private key storage	Y
Trustpoint CLI	Y
Query mode per trustpoint	Y
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	Y
Public-key infrastructure (PKI) query multiple servers	Y
Online Certificate Status Protocol (OCSP)	Y
Optional OCSP nonces	Y
Certificate security attribute-based access control	Y
PKI AAA authorization using entire subject name	Y
PKI local authentication using subject name	Y
Source interface selection for outgoing traffic with certificate authority	Y
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
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

Table 2-1 IPsec Feature Support By Release in All VPN Modes (continued)

Feature Name	Software Release 12.2
	SXI
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
Other **show crypto engine** commands	N
clear crypto engine accelerator counter command	Y
Crypto commands applied to a loopback interface	N
Asymmetric routing (different outside interfaces for encrypted and decrypted traffic of the same tunnel)	N
Policy Based Routing (PBR) on tunnel interface or interface VLAN	N
ACL on tunnel interface	Y
MQC QoS on tunnel interface (service policy)	Y
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
16 K Tunnels (16 K IKE & 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
Dynamic Multipoint VPN Phase 2 (DMVPN) (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)	Y
DMVPN spoke router behind a NAT gateway—tunnel mode	N

Table 2-1 IPsec Feature Support By Release in All VPN Modes (continued)

Feature Name	Software Release 12.2
	SXI
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
ip tcp adjust-mss command for IPv4	Y
Support for Supervisor Engine 2	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	Y
VSPA supported with virtual switching system (VSS)	N
IPv4 header options through IPsec tunnels	N
Invalid SPI recovery	Y
IPsec compression	N
Multilink PPP (MLPPP)	Y
Multilink or dialer interfaces	N
Group Encrypted Transport VPN (GETVPN)	N
IPsec Passive Mode	N
ATM PVC bundle	N

IPsec Features in Crypto-Connect Mode

Table 2-2 displays supported and unsupported IPsec features in crypto-connect mode.

Table 2-2 Features Supported or Unsupported In Crypto-Connect VPN Mode

Feature Name	Software Release 12.2
	SXI
Point-to-point GRE with tunnel protection and VTI	N
Path MTU discovery (PMTUD)	Y
PMTUD with NAT-T	N
IPsec static virtual tunnel interface (sVTI)	N

Table 2-2 Features Supported or Unsupported In Crypto-Connect VPN Mode (continued)

Feature Name	Software Release 12.2
	SXI
The use of VRFs in conjunction with crypto features	N
IPX and Appletalk over point-to-point GRE	Y

IPsec Features in VRF Mode

Table 2-3 displays supported and unsupported IPsec features in VRF mode.

Table 2-3 Features Supported or Unsupported In VRF Mode

Feature Name	Software Release 12.2
	SXI
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
MPLS PE-CE encryption (Tag2IP) with sVTI	Y
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 TACACS	N
IPsec static virtual tunnel interface (sVTI)	Y
Multicast over sVTI	Y
Ingress and egress features (ACL, QOS) on sVTI, GRE/TP, and mGRE tunnel	Y
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)	Y

Table 2-3 Features Supported or Unsupported In VRF Mode (continued)

Feature Name	Software Release 12.2
	SXI
IPv6 IPsec sVTI IPv6-in-IPv6	Y
OSPFv3 with authentication	N
IPv4-in-IPv6, IPv6-in-IPv4	N
Multicast over IPv6 sVTI	N
AH encapsulation over IPv6 sVTI	N
ACL, QOS, NAT, VPN, MPLS, HSRPv6, **tcp adjust-mss** command on IPv6 sVTI	N
Certificates, PMTUD, DPD, PDPD for IPv6	N
IPv6 extension headers on encrypted packets	N
IPv6 extension headers on cleartext packets	Y