Overview of IPsec

IPsec is a framework of open standards developed by the IETF. It provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

- IPsec license must be acquired and installed in the router for IPsec functionality to work. When you enable or disable the IPsec license, reboot is mandatory for the system to function properly.
- NPE images shipped for Cisco routers do not support data plane encryptions. However, control plane encryption is supported with NPE images, with processing done in software, without crypto engine.

The following features are supported for IPsec:

- Internet Key Exchange (IKE) for IPsec
- IKEv1 and IKEv2 Transform sets
- IPSec Virtual Tunnel Interfaces
- Encrypted Preshared Key
- IPSec Dead Peer Detection
- IPsec Anti-replay Window

The following features are supported for PKI:

- Deploying RSA Keys for PKI
- Authorization and Enrollment of Certificates
- CRL support for PKI
- Certificate Enrollment for PKI
- OCSP

For information on understanding and configuring PKI, see Public Key Infrastructure Configuration Guide.

- Information About IPsec, on page 2
- Additional References, on page 11

Information About IPsec

For information about IPSec, see Introduction to Cisco IPsec Technology.

Restrictions For IPsec

- Default routes pointing through the tunnel interface are not supported.
- Default route through VTI is not supported.
- Crypto maps are *not* supported.
- Using the same source IP address for multiple tunnels is not supported, so ensure to use a different IP address for tunnels. For example, consider using a different loopback IP address or a different BDI IP address as the tunnel source IP.
- Packet size greater than 1460 is *not* supported on an IPsec tunnel.
- IPsec traffic acceleration is supported only for UDP-TCP traffic.
- Tunnel mode is only supported.
- Volume-based rekeying is *not* supported.
- IPv6 traffic is *not* supported on IPsec tunnels.
- Multicast Traffic is *not* supported on IPsec tunnels.
- IPsec tunnels are *not* supported on an MPLS cloud.
- IPsec tunnels are *not* supported on vrf lite.
- QoS is *not* supported for IPsec tunnels.
- Maximum number of tunnels that are supported is 32.
- VRF-aware IPsec is *not* supported on Cisco ASR 9xx platforms.
- Hardware encryption is only supported with Advanced Metro IP Access licenses on the router.
- Routing protocols are *not* supported on the tunnel interface.

Restrictions for IPsec on RSP3

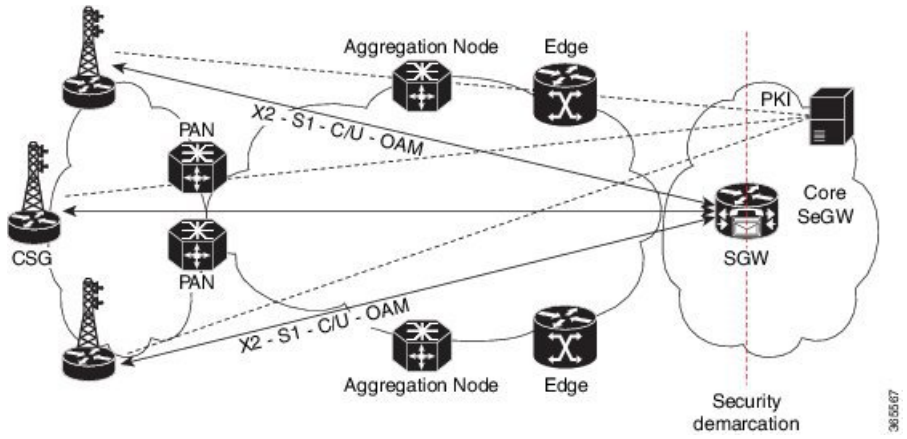
- Tunnel flap is expected after SSO, so minimal traffic drop will be seen.
- Packet with minimum size of 64 bytes (from 128 bytes) might slow down the system to function.
- The overlapping Front Door Virtual Routing and Forwarding (FVRF) feature is not supported.
- When the tunnel starts functioning for the first time, there might be drop in some packets.
- IPsec VPN using VTIs does not display some IPsec security associations and input or output packet VTI counter information (set to zero) for packets that are sent out of the router and received from its VPN peer. The IPsec security associations include encryption or decryption, digestion or verification, and life time of the traffic volume.

- The **show interface tunnel** command does not display input and output packets counter information and there by SNMP statistics information is also not displayed.
- When the **license feature service-offload** command is enabled or disabled, the router has to be reloaded so that the configuration change is updated.
- 32 IPsec tunnels with 2-Mbps traffic on each tunnel are supported.
- The router hangs while performing clear crypto or tunnel flap operations several times with a single path in core. This behavior is not noticed when there is a backup path present in core.
- Default route pointing to IPsec tunnel does not forward traffic. The route with specific prefix should be configured.

Deploying IPsec

In a telecommunication network, IPsec is currently deployed as a centralized security gateway (CSG). The Evolved Nodes (eNB) establish one or more tunnels for the X2, S1-C/U and OAM traffic to flow to the Core Security Gateway (SeGW). The LTE traffic flow is limited. Authentication is provided by PKI.

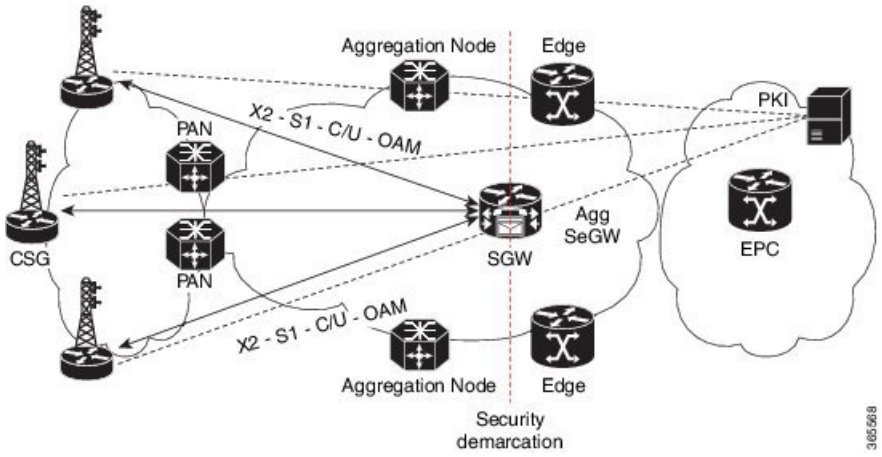
Figure 1: Traffic flowing in a Centralized Security Gateway Network



With a distributed Security Gateway setup, the gateway for traffic to flow is closer to the access layer. This setup allows addressing scale, latency and service availability for LTE and X2 traffic flowing through the tunnels.

The eNB establish one or more IPSec tunnels for the X2, S1-C/-U and OAM traffic flows towards the distributed SeGW. The SeGW addresses scale, latency and service availability. The X2 traffic is terminated on the SeGW, S1-C/U and OAM traffic bypass the distributed SeGW, and are terminated at the centralized Gateway. Authentication is provided by PKI.

Figure 2: Traffic flowing in a Distributed Security Gateway Network



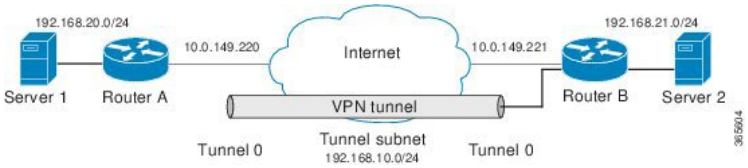
Workflow for Configuring IPsec on the Distributed Gateway

1. Configure IKE
   a. Enable or disable IKE.
   b. Create IKE policies.
   c. (Optional, depends on the IKE parameters) Configure RSA keys.
   d. (Optional, depends on the IKE parameters) Configure Preshared keys.
   e. (Optional, depends on the IKE parameters) Configure Preshared keys using AAA server.
   f. (Optional) Configure IKE mode configuration.
   g. (Optional) Configure IKE extended authentication.
   h. (Optional) Configure Tunnel End point discover.
   i. (Optional) Clear IKE connections.
   j. (Optional) Troubleshoot IKE connections.
2. Configure IPsec
   a. Set global lifetimes for IPSec SAs.
   b. Define transform sets.
3. Configure static virtual tunnel interfaces
   a. Monitor and maintain IPsec.

Example: Configuring IPsec on the Distributed Gateway

The following example configurations describe IPsec configurations on the router.

Figure 3: IPsec Configuratoin



IPsec Configuration using Pre-shared Key

Peer1 configuration using pre-shared key

```
crypto keyring preshare
pre-shared-key address 10.0.149.221 key secret
crypto isakmp policy 1
encr 3des
authentication pre-share
group 5
crypto isakmp profile preshare
keyring preshare
match identity address 10.0.149.221 255.255.255.255
crypto ipsec transform-set AES-SHA1 esp-aes esp-sha-hmac
mode tunnel
crypto ipsec profile ipsec-preshare
set transform-set AES-SHA1
set isakmp-profile preshare
interface Tunnel101
ip address 192.168.10.1 255.255.255.0
tunnel source 10.0.149.220
tunnel mode ipsec ipv4
tunnel destination 10.0.149.221
tunnel protection ipsec profile ipsec-preshare
ip route 192.168.21.0 255.255.255.0 Tunnel101
```

Peer2 configuration using pre-shared key

```
crypto keyring preshare
pre-shared-key address 10.0.149.220 key secret
crypto isakmp policy 1
encr 3des
authentication pre-share
group 5
crypto isakmp profile preshare
keyring preshare
match identity address 10.0.149.220 255.255.255.255
crypto ipsec transform-set AES-SHA1 esp-aes esp-sha-hmac
mode tunnel
crypto ipsec profile ipsec-preshare
set transform-set AES-SHA1
set isakmp-profile preshare

interface Tunnel101
ip address 192.168.10.2 255.255.255.0
tunnel source 10.0.149.221
tunnel mode ipsec ipv4
tunnel destination 10.0.149.220
tunnel protection ipsec profile ipsec-preshare
ip route 192.168.20.0 255.255.255.0 Tunnel101
```

IPsec Configuration using PKI

Peer1 configuration using PKI

Note The CA certificate and ID certificate should be installed from the CA server.

Note The vrf Mgmt-intf should be configured if the CA server is available over the management interface.

```
crypto ikev2 proposal 504
 encryption 3des
 integrity sha1
 group 16
crypto ikev2 policy 504
proposal 504
crypto pki certificate map IKEv2_MAP 1
 issuer-name co cn = ca ( Should be configured according to CA certificate)
crypto pki trustpoint CA
 enrollment url http://<address of CA server>:80
 vrf Mgmt-intf
 revocation-check crl
crypto ikev2 profile 504
 match certificate IKEv2_MAP
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
crypto ipsec transform-set ESP-SHA384-HMAC_504
 esp-des esp-sha384-hmac
 mode tunnel
 crypto ipsec profile ESP-SHA384-HMAC_504
 set transform-set ESP-SHA384-HMAC_504
 set ikev2-profile 504
interface Tunnel504
 ip address 192.168.10.1 255.255.255.0
 tunnel source 10.0.149.220
 tunnel mode ipsec ipv4
 tunnel destination 10.0.149.221
 tunnel protection ipsec profile ESP-SHA384-HMAC_504
ip route 192.168.21.0 255.255.255.0 tunnel504
```

Peer2 configuration using PKI

Note The vrf Mgmt-intf should be configured if the CA server is available over the management interface.

```
crypto ikev2 proposal 504
 encryption 3des
 integrity sha1
 group 16
crypto ikev2 policy 504
proposal 504
crypto pki certificate map IKEv2_MAP 1
 issuer-name co cn = ca   ( Should be configured according to CA certificate )
crypto pki trustpoint CA
 enrollment url http://<Address of CA server >:80
 vrf Mgmt-intf
 revocation-check crl
```

```
crypto ikev2 profile 504
  match certificate IKEv2_MAP
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint CA
crypto ipsec transform-set ESP-SHA384-HMAC_504
 esp-des esp-sha384-hmac
  mode tunnel
crypto ipsec profile ESP-SHA384-HMAC_504
  set transform-set ESP-SHA384-HMAC_504
  set ikev2-profile 504
interface Tunnel504
  ip address 192.168.10.2 255.255.255.0
  tunnel source 10.0.149.221
  tunnel mode ipsec ipv4
  tunnel destination 10.0.149.220
  tunnel protection ipsec profile ESP-SHA384-HMAC_504
 ip route 192.168.20.0 255.255.255.0 tunnel504
```

IPsec Functionality Overview

IPsec provides the following network security services. (In general, the local security policy dictates the use of one or more of these services.)

- Data confidentiality—The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication—The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay—The IPsec receiver can detect and reject replayed packets.

IPsec provides secure *tunnels* between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. (The use of the term *tunnel* in this chapter does not refer to using IPsec in tunnel mode.)

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to 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 (AH or 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 only need to be authenticated, while other data streams must both be encrypted and authenticated.

IKE for IPsec

IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets.

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

IKE has two phases of key negotiation, phase 1 and 2. Phase 1 negotiates a security association between two key peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPsec.

Phase 1 negotiation can occur using main mode or aggressive mode. Main mode tries to protect all information during the negotiation, meaning that no information is available to a potential attacker. When main mode is used, the identities of the two IKE peers are hidden. Although this mode of operation is very secure, it is relatively costly in terms of the time required to complete the negotiation. Aggressive mode takes less time to negotiate keys between peers; however, it gives up some of the security provided by main mode negotiation. For example, the identities of the two parties trying to establish a security association are exposed to an eavesdropper.

Main mode is slower than aggressive mode, but main mode is more secure and more flexible because it can offer an IKE peer more security proposals than aggressive mode. Aggressive mode is less flexible and not as secure, but much faster.

In Cisco IOS software, the two modes are not configurable. The default action for IKE authentication (rsa-sig, rsa-encr, or preshared) is to initiate main mode; however, in cases where there is no corresponding information to initiate authentication, and there is a preshared key associated with the hostname of the peer, Cisco IOS software can initiate aggressive mode. Cisco IOS software will respond in aggressive mode to an IKE peer that initiates aggressive mode.

Prerequisites For IKE

- Ensure ACLs are not blocking UDP port 500.
- The initiating router must not have a certificate associated with the remote peer.

IKE Benefits

IKE automatically negotiates IPsec security associations (SAs) and enables IPsec secure communications without costly manual preconfiguration. Specifically, IKE provides the following benefits:

- Allows you to specify a lifetime for the IPsec SA.
- Allows encryption keys to change during IPsec sessions.
- Allows IPsec to provide antireplay services.
- Permits certification authority (CA) support for a manageable, scalable IPsec implementation.
- Allows dynamic authentication of peers.

IKEv1 Transform Sets

An Internet Key Exchange version 1 (IKEv1) transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation. The default proposal is a collection of commonly used algorithms which are as follows:

```
encryption aes-cbc-128 3des
integrity sha1 md5
group 5 2
```

Although the **crypto ikev2 proposal** command is similar to the **crypto isakmp policy priority** command, the IKEv2 proposal differs as follows:

- An IKEv2 proposal allows configuration of one or more transforms for each transform type.
- An IKEv2 proposal does not have any associated priority.

Note To use IKEv2 proposals in negotiation, they must be attached to IKEv2 policies. If a proposal is not configured, then the default IKEv2 proposal is used with the default IKEv2 policy.

Information About IPsec Virtual Tunnel Interfaces

The use of IPsec VTIs can simplify the configuration process when you need to provide protection for remote access and it provides an alternative to using generic routing encapsulation (GRE) or Layer 2 Tunneling Protocol (L2TP) tunnels for encapsulation. A benefit of using IPsec VTIs is that the configuration does not require static mapping of IPsec sessions to a physical interface. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Because there is a routable interface at the tunnel endpoint, many common interface capabilities can be applied to the IPsec tunnel.

The IPsec VTI allows for the flexibility of sending and receiving both IP unicast and multicast encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted or decrypted when it is forwarded from or to the tunnel interface and is managed by the IP routing table. Using IP routing to forward the traffic to the tunnel interface simplifies the IPsec VPN configuration . Because DVTIs function like any other real interface you can apply quality of service (QoS), firewall, and other security services as soon as the tunnel is active.

The following sections provide details about the IPSec VTI:

Benefits of Using IPsec Virtual Tunnel Interfaces

IPsec VTIs allow you to configure a virtual interface to which you can apply features. Features for clear-text packets are configured on the VTI. Features for encrypted packets are applied on the physical outside interface. When IPsec VTIs are used, you can separate the application of features such as Network Address Translation (NAT), ACLs, and QoS and apply them to clear-text, or encrypted text, or both.

There are two types of VTI interfaces: static VTIs (SVTIs) and dynamic VTIs (DVTIs).

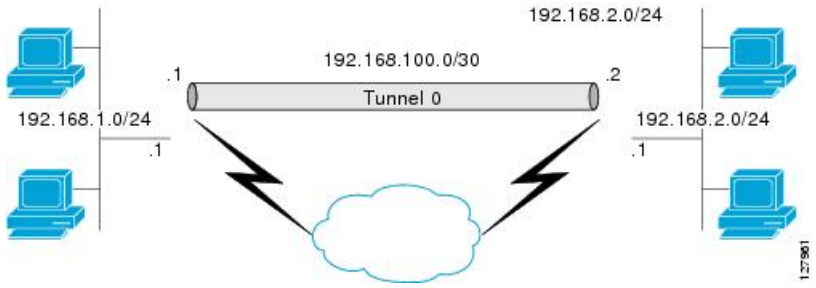
Static Virtual Tunnel Interfaces

SVTI configurations can be used for site-to-site connectivity in which a tunnel provides always-on access between two sites.

Additionally, multiple Cisco IOS software features can be configured directly on the tunnel interface and on the physical egress interface of the tunnel interface. This direct configuration allows users to have solid control on the application of the features in the pre- or post-encryption path.

The figure below illustrates how a SVTI is used.

Figure 4: IPsec SVTI



The IPsec VTI supports native IPsec tunneling and exhibits most of the properties of a physical interface.

Information About Encrypted Preshared Key

Using the Encrypted Preshared Key Feature to Securely Store Passwords

Using the Encrypted Preshared Key feature, you can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key** command with the **password encryption aes** command to configure and enable the password (symmetric cipher AES is used to encrypt the keys). The password (key) configured using the **config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes**command without configuring the **key config-key** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Enabling the Encrypted Preshared Key

The **password encryption aes** command is used to enable the encrypted password.

Information About IPsec Dead Peer DetectionPeriodic Message Option

Using the IPsec Dead Peer Detection Periodic Message Option

With the IPsec Dead Peer Detection Periodic Message Option feature, you can configure your router so that DPD messages are "forced" at regular intervals. This forced approach results in earlier detection of dead peers. For example, if a router has no traffic to send, a DPD message is still sent at regular intervals, and if a peer is dead, the router does not have to wait until the IKE SA times out to find out.

If you want to configure the DPD periodic message option, you should use the **crypto isakmp keepalive** command with the **periodic** keyword. If you do not configure the **periodic** keyword, the router defaults to the on-demand approach.

Note When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Information About IPsec Anti-Replay Window Expanding and Disabling

IPsec Anti-Replay Window

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded when they arrive outside of the 64 packet replay window at the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
IKE, IPsec, and PKI configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z
IKE configuration	*Configuring Internet Key Exchange for IPsec VPNs*
IPsec Virtual Tunnel Interfaces	Security for VPNs with IPsec Configuration Guide
VRF-Aware IPsec	Internet Key Exchange for IPsec VPNs Configuration Guide
Internet Key Exchange for IPsec VPNs	Internet Key Exchange for IPsec VPNs Configuration Guide
Encrypted Preshared Key	Internet Key Exchange for IPsec VPNs Configuration Guide
Suite-B Integrity algorithm type transform configuration	*Configuring Internet Key Exchange Version 2 (IKEv2)*
Suite-B support for certificate enrollment for a PKI	*Configuring Certificate Enrollment for a PKI*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 2402	*IP Authentication Header*
RFC 2403	*The Use of HMAC-MD5-96 within ESP and AH*
RFC 2404	*The Use of HMAC-SHA-1-96 within ESP and AH*
RFC 2405	*The ESP DES-CBC Cipher Algorithm With Explicit IV*
RFC 2406	*IP Encapsulating Security Payload (ESP)*
RFC 2407	*The Internet IP Security Domain of Interpretation for ISAKMP*
RFC 2408	*Internet Security Association and Key Management Protocol (ISAKMP)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html