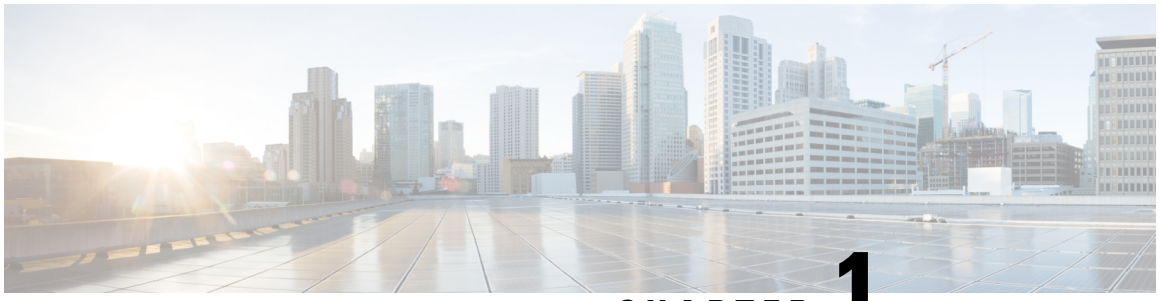
IPsec Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 920 Series)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

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.

Starting with Cisco IOS XE Release 3.18S, IPsec tunnel is supported only on the Cisco ASR920-12SZ-IM routers with payload encryption (PE) images. IPsec requires an IPsec license to function.

- 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

Starting with Cisco IOS XE Release 3.18S, Public Key Infrastructure is supported on the ASR920-12SZ-IM router.

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

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.

  On the ASR 920, hardware encryption is supported when the ASR-920-12SZ-IM boot level is set with both Metro and Advanced Metro IP Access.
- Routing protocols are *not* supported on the tunnel interface.

Restrictions for IPsec on RSP3

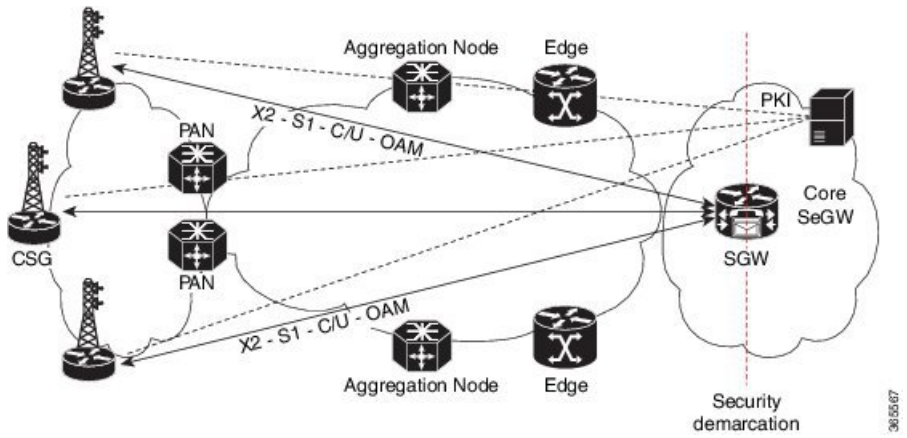
- Tunnel flap is expected after SSO, so minimal traffic drop will be seen.
- Packet with minimum size of 64 bytes (from 128 bytes) might slow down the system to function.
- The overlapping Front Door Virtual Routing and Forwarding (FVRF) feature is not supported.
- When the tunnel starts functioning 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.
- The esp-gsm and esp-gmac transform-sets are *not* supported.

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.

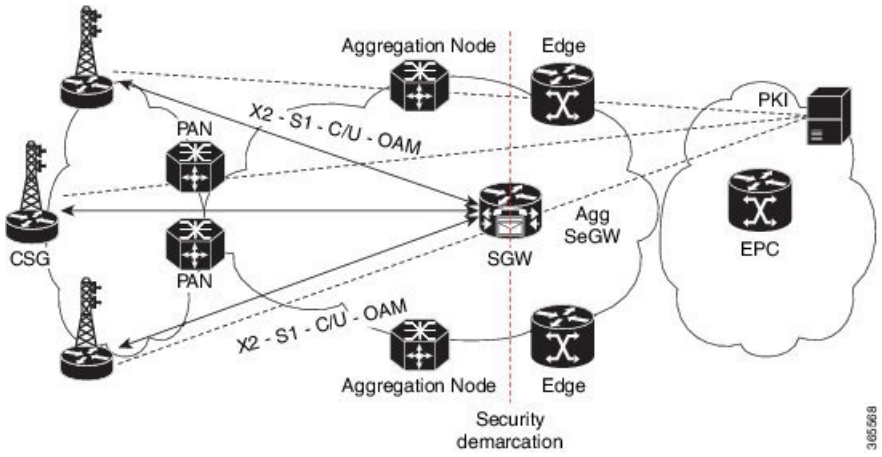
Figure 1: Traffic flowing in a Centralized Security Gateway Network



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



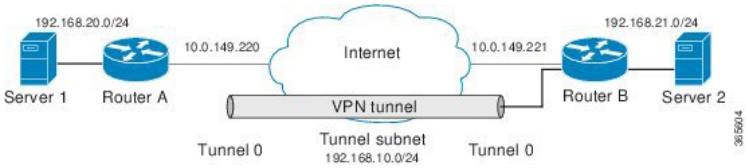
Workflow for Configuring IPsec on the Distributed Gateway

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).

Note Only SVTI is supported.

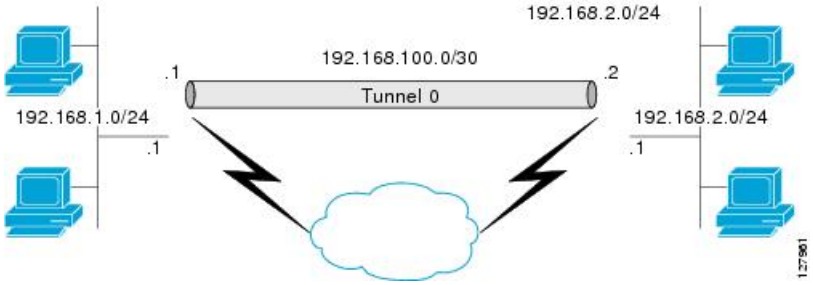
Static Virtual Tunnel Interfaces

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 password-encrypt**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 password-encrypt** 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

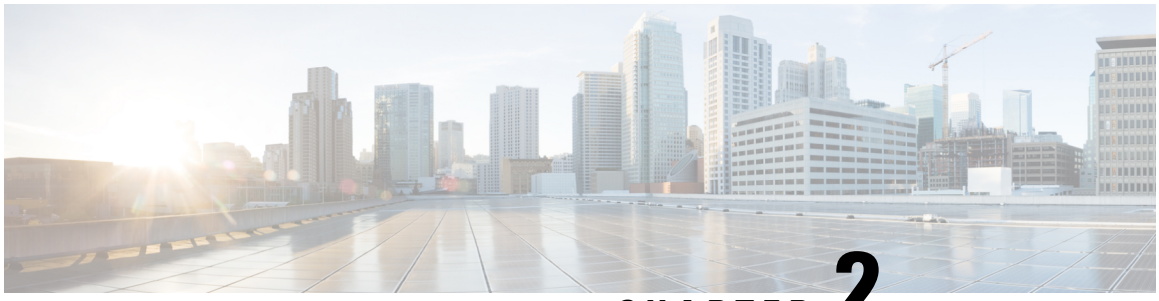
MIBs	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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



CHAPTER 2

Configuring Transform Sets for IKEv1 and IKEv2 Proposals

Perform this task to define a transform set that is to be used by the IPsec peers during IPsec security association negotiations with IKEv1 and IKEv2 proposals.

Configuring Transform Sets for IKEv1

Note Only tunnel mode is supported.

```
enable
configure terminal
crypto ipsec
transform-set aesset esp-aes 256 esp-sha-hmac
mode tunnel
end
```

- Optional Configurations

  Use the **clear crypto sa** command to clear existing IPsec associations in a transform set.

```
Router # clear crypto sa ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  vrf       VRF (Routing/Forwarding) instance
```

  There are complex rules defining the entries that you can use for transform arguments. These rules are explained in the **crypto ipsec transform-set** command. For more information, see About Transform Sets.

Configuring Transform Sets for IKEv2

```
enable
configure terminal
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
mode tunnel
crypto ikev2 proposal proposal-1
encryption aes-cbc-128
integrity sha1
group 14
end
```

Transform Sets for IKEv2 Examples

The following examples show how to configure a proposal:

IKEv2 Proposal with One Transform for Each Transform Type

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14
```

IKEv2 Proposal with Multiple Transforms for Each Transform Type

```
crypto ikev2 proposal proposal-2
encryption aes-cbc-128 aes-cbc-192
integrity sha1 sha256
group 14 15
```

For a list of transform combinations, see Configuring Security for VPNs with IPsec.

IKEv2 Proposals on the Initiator and Responder

The proposal of the initiator is as follows:

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16
```

The proposal of the responder is as follows:

```
Device(config)# crypto ikev2 proposal proposal-2
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14
```

In the scenario, the initiator's choice of algorithms is preferred and the selected algorithms are as follows:

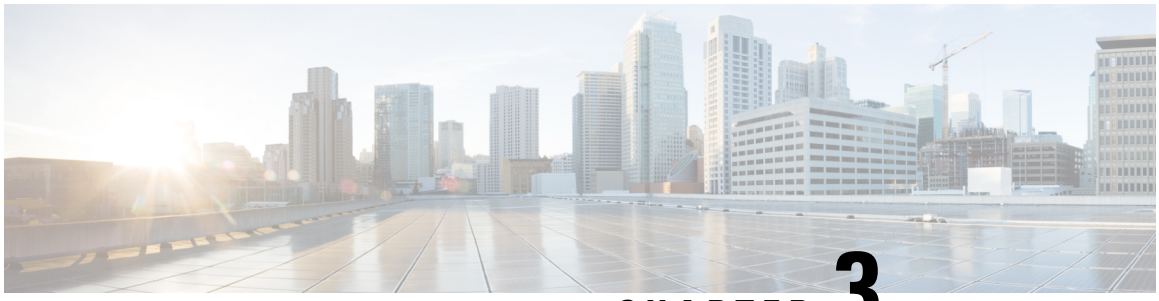
```
encryption aes-cbc-128
integrity sha1
group 14
```

Verifying Transform Sets for IKEv1

```
Router# show crypto ipsec transform-set

Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set ESP-AES256-SHA1: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set ESP-SHA384-HMAC_504: { esp-des esp-sha384-hmac  }
   will negotiate = { Tunnel,  },

Transform set ESP-SHA384-HMAC_30: { esp-des esp-sha384-hmac  }
   will negotiate = { Tunnel,  },

Transform set AES-SHA1: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set ab: { esp-aes esp-sha512-hmac  }
   will negotiate = { Tunnel,  },
```

Verifying Transform Sets for IKEv2

```
Router# show crypto ikev2 proposal
 IKEv2 proposal: 30
     Encryption : 3DES
     Integrity  : SHA96
     PRF        : SHA1
     DH Group   : DH_GROUP_2048_MODP/Group 14
 IKEv2 proposal: default
     Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
     Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
     PRF        : SHA512 SHA384 SHA256 SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
 IKEv2 proposal: prop1
     Encryption : AES-CBC-128
     Integrity  : MD596
     PRF        : MD5
     DH Group   : DH_GROUP_2048_MODP/Group 14
```



CHAPTER 3

Configuring Internet Key Exchange for IPsec VPNs

This module describes how to configure the Internet Key Exchange (IKE) protocol for basic IP Security (IPsec) Virtual Private Networks (VPNs). 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.)

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Creating IKE Policies

Restrictions for configuring AES IKE policy

- IPsec and long keys (the “k9” subsystem) must be supported.
- AES cannot encrypt IPsec and IKE traffic if an acceleration card is present.

```
enable
configure terminal
crypto isakmp policy 10
```

```
encryption aes 256
hash sha
authentication pre-share
group 14
end
```

Troubleshooting Tips

- Clear (and reinitialize) IPsec SAs by using the **clear crypto sa** EXEC command.

Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command in the Cisco IOS Security Command Reference.

- The default policy and default values for configured policies do not show up in the configuration when you issue the **show running-config** command. To display the default policy and any default values within configured policies, use the **show crypto isakmp policy** command.
- Any IPsec transforms or IKE encryption methods that the current hardware does not support should be disabled; they are ignored whenever an attempt to negotiate with the peer is made.

If a user enters an IPsec transform or an IKE encryption method that the hardware does not support, a warning message will be generated. These warning messages are also generated at boot time. When an encrypted card is inserted, the current configuration is scanned. If any IPsec transforms or IKE encryption methods are found that are not supported by the hardware, a warning message will be generated.

Configuring IKE Authentication

After you have created at least one IKE policy in which you specified an authentication method (or accepted the default method), you need to configure an authentication method. IKE policies cannot be used by IPsec until the authentication method is successfully configured.

Note Before configuring IKE authentication, you must have configured at least one IKE policy, which is where the authentication method was specified (or RSA signatures was accepted by default).

To configure IKE authentication, you should perform one of the following tasks, as appropriate:

Configuring RSA Keys Manually for RSA Encrypted Nonces

Note This task can be performed only if a CA is not in use.

```
enable
configure terminal
crypto key generate rsa general-keys modulus 360
crypto key generate ec keysize 256 label Router_1_Key
end
```

Optional Configuration using Named Key

```
enable
configure terminal
crypto key pubkey-chain rsa
named-key otherpeer.example.com
address 10.5.5.1
key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
```

Optional Configuration using Addresses Key

```
enable
configure terminal
crypto key pubkey-chain rsa
addressed-key 10.1.1.2 encryption
address 10.5.5.1
key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
```

Configuring Preshared Keys

Note Preshared keys do not scale well with a growing network.

Restrictoins for Mask Preshared Keys

- The SA cannot be established between the IPsec peers until all IPsec peers are configured for the same preshared key.
- The mask preshared key must be distinctly different for remote users requiring varying levels of authorization. A new preshared key should be configured for each level of trust and correct keys must be assigned to the correct parties. Otherwise, an untrusted party may obtain access to protected data.

```
enable
configure terminal
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth
crypto isakmp key sharedkeystring address 10.0.0.1
end
```

Configuring IKE Mode Configuration

```
enable
configure terminal
```

```
ip local pool pool1 172.16.23.0 172.16.23.255
crypto isakmp client configuration address-pool local pool1
end
```

Configuration Examples for an IKE Configuration

Example: Creating IKE Policies

This section contains the following examples, which show how to configure an AES IKE policy and a 3DES IKE policy.

Note Cisco no longer recommends using 3DES; instead, you should use AES. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Example: Creating an AES IKE Policy

The following example is sample output from the **show running-config**command. In this example, the AES 256-bit key is enabled.

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport

.
.
.
```

Example: Creating 3DES IKE Policies

This example creates two IKE policies, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
!
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

In the example, the encryption DES of policy default would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

If the **show crypto isakmp policy**command is issued with this configuration, the output is as follows:

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

Note that although the output shows “no volume limit” for the lifetimes, you can configure only a time lifetime (such as 86,400 seconds); volume-limit lifetimes are not configurable.

Example: Configuring IKE Authentication

The following example shows how to manually specify the RSA public keys of two IPsec peer-- the peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys:

```
crypto key pubkey-chain rsa
 named-key otherpeer.example.com
 address 10.5.5.1
 key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
```

```
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
exit
addressed-key 10.1.1.2 encryption
key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
exit
addressed-key 10.1.1.2 signature
key-string
0738BC7A 2BC3E9F0 679B00FE 53987BCC
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
exit
exit
```

Verifying IKE Policies

```
Router# show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

Verifying RSA Keys

```
Router# show crypto key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate

Code Usage         IP-Address/VRF         Keyring          Name
C    Signing                            default         cn=Cisco Licensing Root CA,o=Cisco
C    Signing                              default          cn=CA
C    Signing                              default          cn=Cisco Root CA M1,o=Cisco
C    Signing                              default          cn=Cisco Root CA 2048,o=Cisco
Systems
C    Signing                             default         cn=Cisco Manufacturing CA,o=Cisco
 Systems
C    Signing                              default          ou=Class 3 Public Primary
Certification Authority,o=VeriSign, Inc.,c=US
C    Signing                              default          cn=Cisco Root CA M2,o=Cisco
C    Signing                              default          cn=Cisco Manufacturing CA
SHA2,o=Cisco
C    Signing                              default          cn=Licensing Root - DEV,o=Cisco
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands: complete command syntax, command mode, command history, 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
IPsec configuration	Configuring Security for VPNs with IPsec
IKE Version 2	Configuring Internet Key Exchange Version 2
Configuring RSA keys to obtain certificates from a CA	Deploying RSA Keys Within a PKI
Suite-B ESP transforms	Configuring Security for VPNs with IPsec
Suite-B support for certificate enrollment for a PKI	Configuring Certificate Enrollment for a PKI

Standards

Standards	Title
None	--

MIBs

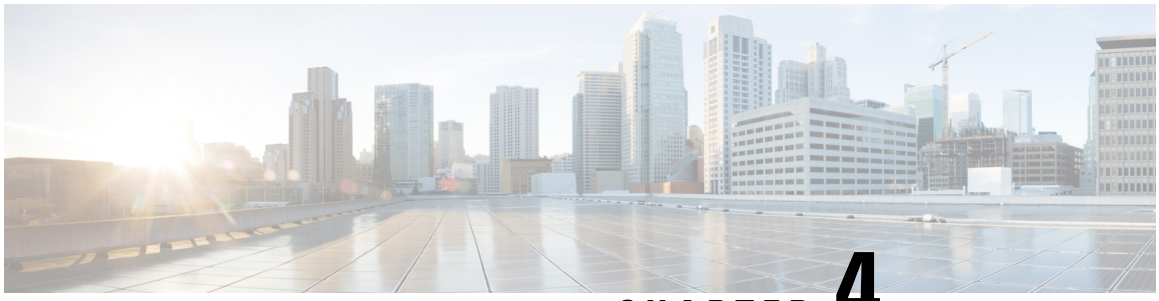
MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409	The Internet Key Exchange (IKE)
RFC 2412	The OAKLEY Key Determination Protocol

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



CHAPTER 4

IPsec Virtual Tunnel Interfaces

IPsec virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify the configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Restrictions for IPsec Virtual Tunnel Interfaces

Fragmentation

Fragmentation is not supported over IPsec tunnel. You can choose to set the lower MTU on hosts to avoid packet fragments or choose to fragment the packets on any device.

IPsec Transform Set

The IPsec transform set must be configured in tunnel mode only.

IKE Security Association

The Internet Key Exchange (IKE) security association (SA) is bound to the VTI.

IPsec SA Traffic Selectors

Static VTIs (SVTIs) support only a single IPsec SA that is attached to the VTI interface. The traffic selector for the IPsec SA is always “IP any any.”

By default, Static VTIs (SVTIs) support only a single IPSec SA that is attached to the virtual tunnel interface. The traffic selector for the IPsec SA is always “IP any any”.

IPv4

This feature supports SVTIs that are configured to encapsulate IPv4 packets .

Tunnel Protection

Do not configure the **shared** keyword when using the **tunnel mode ipsec ipv4** command for IPsec IPv4 mode.

Traceroute

The traceroute function with crypto offload on VTIs is not supported.

VxLAN GPE Tunnel Interface

The VxLAN GPE Tunnel Interface cannot use the same source interface as IPsec VTI.

How to Configure IPsec Virtual Tunnel Interfaces

Configuring Static IPsec Virtual Tunnel Interfaces

```
enable
configure terminal
crypto IPsec profile PROF
set transform-set tset
exit
interface tunnel 0
ip address 10.1.1.1 255.255.255.0
tunnel mode ipsec ipv4
tunnel source loopback 0
tunnel destination 172.16.1.1
tunnel protection IPsec profile PROF
end
```

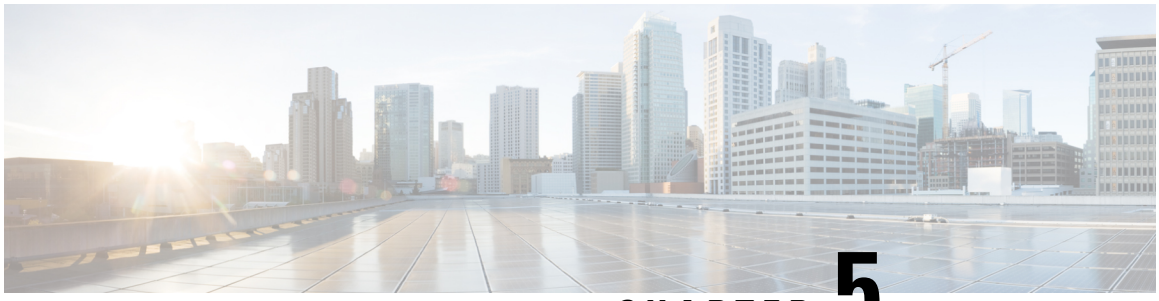
Configuration Examples for IPsec Virtual Tunnel Interfaces

Example: Verifying IPsec Static Virtual Tunnel Interface

```
Router# show interface tunnel 130

Tunnel130 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.130.1/24
  MTU 17878 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 6.6.6.130, destination 7.7.7.130
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1438 bytes
  Tunnel transmit bandwidth 8000 (kbps)
```

```
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "test")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d22h
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
Router# show crypto session

Crypto session current status

Interface: Tunnel30
Profile: 30
Session status: UP-ACTIVE
Peer: 1.1.1.50 port 500
  Session ID: 167
  IKEv2 SA: local 3.1.1.50/500 remote 1.1.1.50/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel31
Profile: 30
Session status: UP-ACTIVE
Peer: 1.1.1.51 port 500
  Session ID: 2
  IKEv2 SA: local 3.1.1.51/500 remote 1.1.1.51/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel40
Profile: 40
Session status: UP-ACTIVE
Peer: 40.40.40.2 port 500
  Session ID: 0
  IKEv1 SA: local 40.40.40.1/500 remote 40.40.40.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Interface: Tunnel41
Profile: 41
Session status: UP-ACTIVE
Peer: 41.41.41.2 port 500
  Session ID: 0
  IKEv1 SA: local 41.41.41.1/500 remote 41.41.41.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
.
.
!

Router# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
       ia - IS-IS inter area, * - candidate default, U - per-user static ro
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 2 subnets
S        1.1.1.50 [1/0] via 101.101.101.2
S        1.1.1.51 [1/0] via 101.101.101.2
      3.0.0.0/32 is subnetted, 2 subnets
C        3.1.1.50 is directly connected, Loopback30
C        3.1.1.51 is directly connected, Loopback31
      6.0.0.0/32 is subnetted, 65 subnets
C        6.6.6.100 is directly connected, Loopback100
C        6.6.6.101 is directly connected, Loopback101
C        6.6.6.102 is directly connected, Loopback102
C        6.6.6.103 is directly connected, Loopback103

.
.
!
```



CHAPTER 5

Encrypted Preshared Key

The Encrypted Preshared Key feature allows you to securely store plain text passwords in type 6 (encrypted) format in NVRAM.

How to Configure an Encrypted Preshared Key

Configuring Preshared Keys

Note Preshared keys do not scale well with a growing network.

Restrictoins for Mask Preshared Keys

- The SA cannot be established between the IPsec peers until all IPsec peers are configured for the same preshared key.
- The mask preshared key must be distinctly different for remote users requiring varying levels of authorization. A new preshared key should be configured for each level of trust and correct keys must be assigned to the correct parties. Otherwise, an untrusted party may obtain access to protected data.

```
enable
configure terminal
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth
crypto isakmp key sharedkeystring address 10.0.0.1
end
```

Troubleshooting Tips

If you see the warning message “ciphertext >[for username bar>] is incompatible with the configured master key,” you have entered or cut and pasted cipher text that does not match the master key or there is no master key. (The cipher text will be accepted or saved.) The warning message will allow you to locate the broken configuration line or lines.

Monitoring Encrypted Preshared Keys

```
enable
configure terminal
password logging
end
```

The following **password logging** debug output shows that a new master key has been configured and that the keys have been encrypted with the new master key.

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas
Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

Configuring ISAKMP Preshared Key

```
enable
configure terminal
crypto isakmp key cisco address 10.2.3.4
crypto isakmp key mykey hostname mydomain.com
end
```

Configuring ISAKMP Preshared Key in ISAKMP Keyrings

```
enable
configure terminal
crypto keyring mykeyring
pre-shared-key address 10.2.3.5 key cisco
pre-shared-key hostname mydomain.com key cisco
end
```

Configuring ISAKMP Aggressive Mode

```
enable
configure terminal
isakmp peer ip-address 10.2.3.4
set aggressive-mode client-endpoint fqdn cisco.com
set aggressive-mode password cisco
end
```

Configuration Examples for Encrypted Preshared Key

Encrypted Preshared Key Example

The following is an example of a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
 crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# password encryption aes

Router (config)# key config-key password-encrypt

New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

No Previous Key Present Example

In the following configuration example, no previous key is present:

```
Router (config)#key config-key password-encrypt testkey 123
```

Key Already Exists Example

In the following configuration example, a key already exists:

```
Router (config)# key config-key password-encrypt testkey123
Old key:
Router (config)#
```

Key Already Exists But the User Wants to Key In Interactively Example

In the following configuration example, the user wants to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts will show on your screen if you enter the **key config-key password-encrypt** command and press the enter key to get into interactive mode.

```
Router (config)#  key config-key password-encrypt
Old key:
New key:
Confirm key:
```

No Key Present But the User Wants to Key In Interactively Example

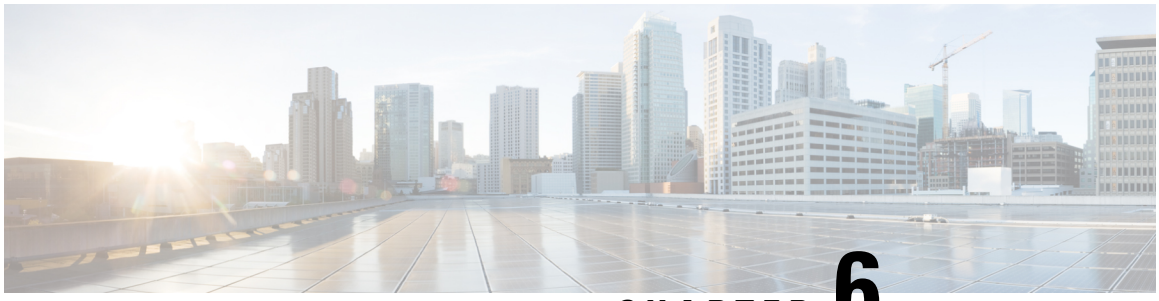
In the following example, the user wants to key in interactively, but no key is present. The New key and Confirm key prompts will show on your screen if you are in interactive mode.

```
Router (config)# key config-key password-encrypt

New key:
Confirm key:
```

Removal of the Password Encryption Example

In the following configuration example, the user wants to remove the encrypted password. The "WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:" prompt will show on your screen if you are in interactive mode.

```
Router (config)# no key config-key password-encrypt
WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion
 ? [yes/no]: y
```



CHAPTER 6

IPsec Dead Peer Detection Periodic Message Option

The IPsec Dead Peer Detection Periodic Message Option feature is used to configure the router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Prerequisites for IPsec Dead Peer Detection PeriodicMessage Option

Before configuring the IPsec Dead Peer Detection Periodic Message Option feature, you should have the following:

- Familiarity with configuring IP Security (IPsec).

Restrictions for IPsec Dead Peer Detection PeriodicMessage Option

Using periodic DPD potentially allows the router to detect an unresponsive IKE peer with better response time when compared to on-demand DPD. However, use of periodic DPD incurs extra overhead. When communicating to large numbers of IKE peers, you should consider using on-demand DPD instead.

How to Configure IPsec Dead Peer Detection PeriodicMessage Option

Configuring a Periodic DPD Message

To configure a periodic DPD message, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive** *seconds* [*retry-seconds*] [**periodic** | **on-demand**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp keepalive** *seconds* [*retry-seconds*] [**periodic** | **on-demand**] **Example:** `Router (config)# crypto isakmp keepalive 10 periodic`	Allows the gateway to send DPD messages to the peer. • *seconds* --When the **periodic** keyword is used, this argument is the number of seconds between DPD messages; the range is from 10 to 3600 seconds. When the **on-demand** keyword is used, this argument is the number of seconds during which traffic is not received from the peer before DPD retry messages are sent if there is data (IPSec) traffic to send; the range is from 10 to 3600 seconds. **Note** If you do not specify a time interval, an error message appears. • *retry-seconds* --(Optional) Number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry

	Command or Action	Purpose
		message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Note** To configure DPD with IPsec High Availability (HA), the recommendation is to use a value other than the default (which is 2 seconds). A keepalive timer of 10 seconds with 5 retries seems to work well with HA because of the time that it takes for the router to get into active mode. • **periodic** --(Optional) DPD messages are sent at regular intervals. • **on-demand** --(Optional) The default behavior. DPD retries are sent on demand. **Note** Because this option is the default, the **on-demand** keyword does not appear in configuration output.

Verifying That DPD Is Enabled

DPD allows the router to clear the IKE state when a peer becomes unreachable. If DPD is enabled and the peer is unreachable for some time, you can use the **clear crypto session** command to manually clear IKE and IPsec SAs.

The **debug crypto isakmp** command can be used to verify that DPD is enabled.

SUMMARY STEPS

1. **enable**
2. **clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*]
3. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*] **Example:** `Router# clear crypto session`	Deletes crypto sessions (IPsec and IKE SAs).
Step 3	**debug crypto isakmp** **Example:** `Router# debug crypto isakmp`	Displays messages about IKE events.

Configuration Examples for IPsec Dead Peer DetectionPeriodic Message Option

Site-to-Site Setup with Periodic DPD Enabled Example

The following configurations are for a site-to-site setup with periodic DPD enabled. The configurations are for the IKE Phase 1 policy and for the IKE preshared key.

IKE Phase 1 Policy

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
```

IKE Preshared Key

```
crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac

!
!
interface GigabitEternet 0/0
  ip address 10.1.32.14 255.255.255.0
  speed auto

!
```

Additional References

Related Documents

Related Topic	Document Title
Configuring IPsec	Configuring Security for VPNs with IPsec
IPsec commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	--

MIBs

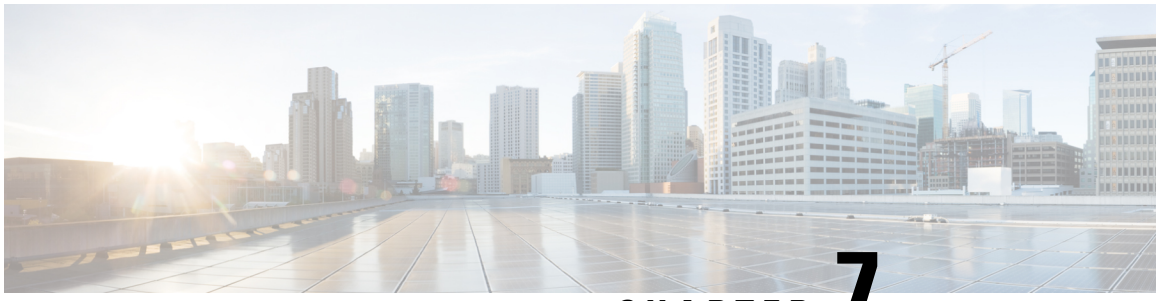
MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
DPD conforms to the Internet draft "draft-ietf-ipsec-dpd-04.txt," which is pending publication as an Informational RFC (a number has not yet been assigned).	--

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



CHAPTER 7

IPsec Anti-Replay Window Expanding and Disabling

Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. 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.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Prerequisites for IPsec Anti-Replay Window Expanding and Disabling

- Before configuring this feature, you should have already created a crypto profile.

How to Configure IPsec Anti-Replay Window Expanding and Disabling

Configuring IPsec Anti-Replay Window Expanding and Disabling Globally

To configure IPsec Anti-Replay Window: Expanding and Disabling globally (so that it affects all SAs that are created), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size** [*N*]
4. **crypto ipsec security-association replay disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec security-association replay window-size** [*N*] **Example:** `Router (config)# crypto ipsec security-association replay window-size 256`	Sets the size of the SA replay window globally. **Note** Configure this command or the **crypto ipsec security-association replay disable** command. The two commands are not used at the same time.
Step 4	**crypto ipsec security-association replay disable** **Example:** `Router (config)# crypto ipsec security-association replay disable`	Disables checking globally. **Note** Configure this command or the **crypto ipsec security-association replay window-size** command. The two commands are not used at the same time.

Configuration Examples for IPsec Anti-Replay Window Expanding and Disabling

Global Expanding and Disabling of an Anti-Replay Window Example

The following example shows that the anti-replay window size has been set globally to 1024:

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
  encryption aes
  authentication pre-share
  group 14
crypto isakmp key cisco123 address 192.165.201.2
crypto ipsec security-association replay window-size 1024
crypto ipsec transform-set basic esp-aes esp-sha-hmac

!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!

!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101 remark
 Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Security Command Reference
IP security and encryption	Configuring Security for VPNs with IPsec

MIBs

MIBs	MIBs Link
None.	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
None.	--

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