



Implementing IPsec in IPv6 Security

First Published: November 3, 2003

Last Updated: October 31, 2005

Cisco IOS IPv6 security features for your Cisco networking devices can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

Cisco IOS IPsec functionality provides network data encryption at the IP packet level, offering a robust, standards-based security solution. IPsec provides data authentication and anti-replay services in addition to data confidentiality services.

IPsec is a mandatory component of IPv6 specification. OSPF for IPv6 provides IPsec authentication support and protection, and IPv6 IPsec tunnel mode and encapsulation is used to protect IPv6 unicast and multicast traffic.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Implementing IPsec in IPv6 Security](#)” section on page 20 or the “Start Here: Cisco IOS Software Release Specifics for IPv6 Features” document.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Implementing IPsec for IPv6 Security, page 2](#)
- [Information About Implementing IPsec for IPv6 Security, page 2](#)
- [How to Implement IPsec for IPv6 Security, page 4](#)
- [Configuration Examples for IPsec for IPv6 Security, page 18](#)
- [Additional References, page 19](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for Implementing IPsec in IPv6 Security, page 20](#)

Prerequisites for Implementing IPsec for IPv6 Security

- You should be familiar with IPv4. Refer to the publications referenced in the “[Related Documents](#)” section for IPv4 configuration and command reference information.
- You should be familiar with IPv6 addressing and basic configuration. Refer to the *Implementing Basic Connectivity for IPv6* module for more information.

Information About Implementing IPsec for IPv6 Security

To implement security features for IPv6, you need to understand the following concepts:

- [OSPF for IPv6 Authentication Support with IPsec, page 2](#)
- [IPsec for IPv6, page 2](#)

OSPF for IPv6 Authentication Support with IPsec

In order to ensure that OSPF for IPv6 packets are not altered and re-sent to the router, causing the router to behave in a way not desired by its managers, OSPF for IPv6 packets must be authenticated. OSPF for IPv6 uses the IP Security (IPsec) secure socket application program interface (API) to add authentication to OSPF for IPv6 packets. This API has been extended to provide support for IPv6.

OSPF for IPv6 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPF for IPv6.

In OSPF for IPv6, authentication fields have been removed from OSPF headers. When OSPF runs on IPv6, OSPF relies on the IPv6 authentication header (AH) and IPv6 encapsulating security payload (ESP) to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH and ESP extension headers can be used to provide authentication and confidentiality to OSPF for IPv6.

To configure IPsec, users configure a security policy, which is a combination of the security policy index (SPI) and the key (the key creates and validates the Message Digest 5 [MD5] value). IPsec for OSPF for IPv6 can be configured on an interface or on an OSPF area. For higher security, users should configure a different policy on each interface configured with IPsec. If a user configures IPsec for an OSPF area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPF for IPv6, IPsec is invisible to the user.

For information about configuring IPsec on OSPF in IPv6, see the *Implementing OSPF for IPv6* module.

IPsec for IPv6

IP Security, or IPsec, is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provide security for 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 provides the following optional network security services. In general, local security policy will dictate the use of one or more of these services:

- Data confidentiality—The IPsec sender can encrypt packets before sending 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 IPsec packets sent. This service depends upon the data integrity service.
- Antireplay—The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be sent across a public network without observation, modification, or spoofing. IPsec functionality is similar in both IPv6 and IPv4; however, site-to-site tunnel mode only is supported in IPv6.

In IPv6, IPsec is implemented using the AH authentication header and the ESP extension header. The authentication header provides integrity and authentication of the source. It also provides optional protection against replayed packets. The authentication header protects the integrity of most of the IP header fields and authenticates the source through a signature-based algorithm. The ESP header provides confidentiality, authentication of the source, connectionless integrity of the inner packet, antireplay, and limited traffic flow confidentiality.

The Internet Key Exchange (IKE) protocol is a key management protocol standard that is used in conjunction with IPsec. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

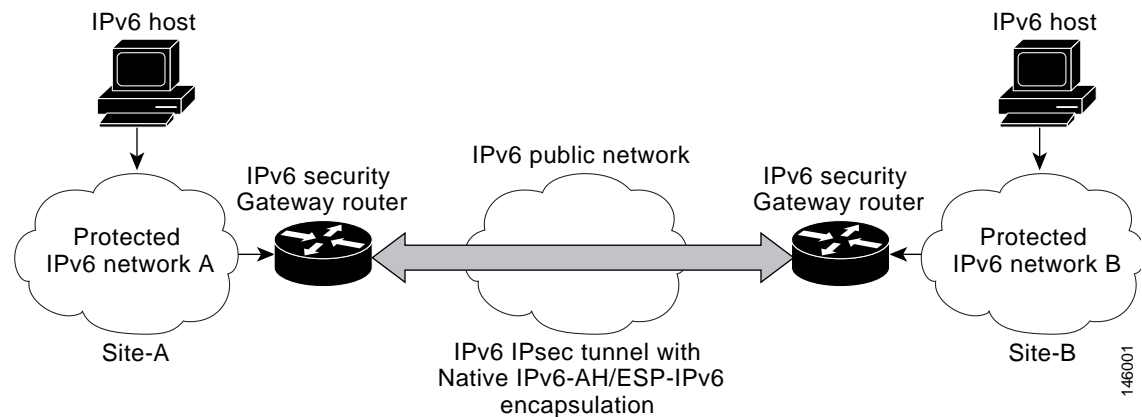
IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) (see [Figure 1](#)). This functionality is similar to the security gateway model using IPv4 IPsec protection.

IPv6 IPsec Site-to-Site Protection Using Virtual Tunnel Interface

The IPsec virtual tunnel interface (VTI) provides site-to-site IPv6 crypto protection of IPv6 traffic. Native IPv6 IPsec encapsulation is used to protect all types of IPv6 unicast and multicast traffic.

The IPsec VTI allows IPv6 routers to work as security gateways, establish IPsec tunnels between other security gateway routers, and provide crypto IPsec protection for traffic from internal networks when it is sent across the public IPv6 Internet (see [Figure 1](#)). This functionality is similar to the security gateway model using IPv4 IPsec protection.

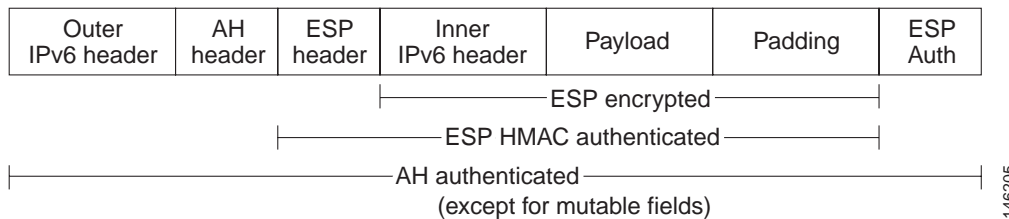
Figure 1 IPsec Tunnel Interface for IPv6



When the IPsec tunnel is configured, IKE and IPsec security associations (SAs) are negotiated and set up before the line protocol for the tunnel interface is changed to the UP state. The remote IKE peer is the same as the tunnel destination address; the local IKE peer will be the address picked from tunnel source interface which has the same IPv6 address scope as tunnel destination address.

Figure 2 shows the IPsec packet format.

Figure 2 IPv6 IPsec Packet Format



For further information on IPsec VTI, see the *IPsec Virtual Tunnel Interface* module in Cisco IOS Release 12.3(14)T.

How to Implement IPsec for IPv6 Security

The tasks in the following sections explain how to configure IPsec for IPv6:

- [Configuring a VTI for Site-to-Site IPv6 IPsec Protection, page 4](#)
- [Verifying IPsec Tunnel Mode Configuration, page 12](#)
- [Troubleshooting IPsec for IPv6 Configuration and Operation, page 14](#)

Configuring a VTI for Site-to-Site IPv6 IPsec Protection

The following tasks describe how to configure an IPsec VTI for site-to-site IPsec protection of IPv6 unicast and multicast traffic. This feature allows the use of IPv6 IPsec encapsulation to protect IPv6 traffic.

- [Creating an IKE Policy and a Preshared Key in IPv6, page 4](#) (Required)
- [Configuring ISAKMP Aggressive Mode, page 7](#) (Optional)
- [Configuring an IPsec Transform Set and IPsec Profile, page 8](#) (Required)
- [Configuring an ISAKMP Profile in IPv6, page 9](#) (Required)
- [Configuring IPv6 IPsec VTI, page 10](#) (Required)

Creating an IKE Policy and a Preshared Key in IPv6

Because IKE negotiations must be protected, each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.

After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

You can configure multiple, prioritized policies on each peer—each with a different combination of parameter values. However, 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).

**Note**

If you are interoperating with a device that supports only one of the values for a parameter, your choice is limited to the value supported by the other device. Aside from this limitation, there is often a trade-off between security and performance, and many of these parameter values represent such a trade-off. You should evaluate the level of security risks for your network and your tolerance for these risks.

IKE Peers Agreeing Upon a Matching IKE Policy

When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime that is less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used.)

If a match is found, IKE will complete negotiation, and IPsec security associations will be created. If no acceptable match is found, IKE refuses negotiation and IPsec will not be established.

**Note**

Depending on which authentication method is specified in a policy, additional configuration might be required. If a peer's policy does not have the required companion configuration, the peer will not submit the policy when attempting to find a matching policy with the remote peer.

ISAKMP Identity for Preshared Keys

You should set the ISAKMP identity for each peer that uses preshared keys in an IKE policy.

When two peers use IKE to establish IPsec SAs, each peer sends its identity to the remote peer. Each peer sends either its hostname or its IPv6 address, depending on how you have set the ISAKMP identity of the router.

By default, a peer's ISAKMP identity is the IPv6 address of the peer. If appropriate, you could change the identity to be the peer's hostname instead. As a general rule, set the identities of all peers the same way—either all peers should use their IPv6 addresses or all peers should use their hostnames. If some peers use their hostnames and some peers use their IPv6 addresses to identify themselves to each other, IKE negotiations could fail if the identity of a remote peer is not recognized and a DNS lookup is unable to resolve the identity.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy *priority***
4. **authentication {rsa-sig | rsa-encr | pre-share}**

5. **hash** {**sha** | **md5**}
6. **group** {**1** | **2** | **5**}
7. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
8. **lifetime** *seconds*
9. **exit**
10. **crypto isakmp key** *password-type keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address/ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
11. **crypto keyring** *keyring-name* [**vrf** *fvrif-name*]
12. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}}
key *key*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp policy <i>priority</i> Example: Router(config)# crypto isakmp policy 15	Defines an IKE policy, and enters ISAKMP policy configuration mode. Policy number 1 indicates the policy with the highest priority. The smaller the <i>priority</i> argument value, the higher the priority.
Step 4	authentication { rsa-sig rsa-encr pre-share } Example: Router(config-isakmp-policy)# authentication pre-share	Specifies the authentication method within an IKE policy. The rsa-sig and rsa-encr keywords are not supported in IPv6.
Step 5	hash { sha md5 } Example: Router(config-isakmp-policy)# hash md5	Specifies the hash algorithm within an IKE policy.
Step 6	group { 1 2 5 } Example: Router(config-isakmp-policy)# group 2	Specifies the Diffie-Hellman group identifier within an IKE policy.
Step 7	encryption { des 3des aes aes 192 aes 256 } Example: Router(config-isakmp-policy)# encryption 3des	Specifies the encryption algorithm within an IKE policy.

	Command or Action	Purpose
Step 8	lifetime <i>seconds</i> Example: Router(config-isakmp-policy)# lifetime 43200	Specifies the lifetime of an IKE SA. Setting the IKE lifetime value is optional.
Step 9	exit Example: Router(config-isakmp-policy)# exit	Enter this command to exit ISAKMP policy configuration mode and enter global configuration mode.
Step 10	crypto isakmp key <i>enc-type-digit keystring</i> {address peer-address [mask] ipv6 {ipv6-address/ipv6-prefix} hostname hostname} [no-xauth] Example: Router(config)# crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128	Configures a preshared authentication key.
Step 11	crypto keyring <i>keyring-name [vrf fvrf-name]</i> Example: Router(config)# crypto keyring keyring1	Defines a crypto keyring to be used during IKE authentication.
Step 12	pre-shared-key {address address [mask] hostname hostname ipv6 {ipv6-address ipv6-prefix}} key key Example: Router (config-keyring)# pre-shared-key ipv6 3FFE:2002::A8BB:CFF:FE01:2C02/128	Defines a preshared key to be used for IKE authentication.

Configuring ISAKMP Aggressive Mode

This optional task describes how to configure ISAKMP aggressive mode.



Note

You likely do not need to configure aggressive mode in a site-to-site scenario. The default mode is typically used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer** **{address {ipv4-address | ipv6 ipv6-address ipv6-prefix-length} | hostname fqdn-hostname}**
4. **set aggressive-mode client-endpoint** **{client-endpoint | ipv6 ipv6-address}**

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 peer { address { <i>ipv4-address</i> ipv6 <i>ipv6-address ipv6-prefix-length</i> } hostname <i>fqdn-hostname</i> } Example: Router(config)# crypto isakmp peer address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128	Enables an IPsec peer for IKE querying for tunnel attributes.
Step 4	set aggressive-mode client-endpoint { <i>client-endpoint</i> ipv6 <i>ipv6-address</i> } Example: Router(config-isakmp-peer)# set aggressive mode client-endpoint ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128	Defines the remote peer's IPv6 address, which will be used by aggressive mode negotiation. The remote peer's address is usually the client side's end-point address.

Configuring an IPsec Transform Set and IPsec Profile

This task describes how to configure an IPsec transform set. A transform set is a combination of security protocols and algorithms that is acceptable to the IPsec routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
4. **crypto ipsec profile** *name*
5. **set transform-set** *transform-set-name* [*transform-set-name2*...*transform-set-name6*]

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 transform-set <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i>] [<i>transform3</i>] [<i>transform4</i>] Example: Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des	Defines a transform set, and places the router in crypto transform configuration mode.
Step 4	crypto ipsec profile <i>name</i> Example: Router(config)# crypto ipsec profile profile0	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.
Step 5	set transform-set <i>transform-set-name</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router (config-crypto-transform)# set-transform-set myset0	Specifies which transform sets can be used with the crypto map entry.

Configuring an ISAKMP Profile in IPv6

This optional task describes how to configure an ISAKMP profile in IPv6.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name* [**accounting** *aaalist*]
4. **self-identity** {**address** | **address ipv6**} | **fqdn** | **user-fqdn** *user-fqdn*}
5. **match identity** {**group** *group-name* | **address** {*address* [*mask*] [*fvrfl*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

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 profile <i>profile-name</i> [accounting <i>aaalist</i>] Example: Router(config)# crypto ipsec profile profile1	Defines an ISAKMP profile and audits IPsec user sessions.
Step 4	self-identity { address address ipv6] fqdn user-fqdn <i>user-fqdn</i> } Example: Router(config-isakmp-profile)# self-identity address ipv6	Defines the identity that the local IKE uses to identify itself to the remote peer.
Step 5	match identity { group <i>group-name</i> address { address [<i>mask</i>] [<i>fvrf</i>] ipv6 <i>ipv6-address</i> } host <i>host-name</i> host domain <i>domain-name</i> user <i>user-fqdn</i> user domain <i>domain-name</i> } Example: Router(config-isakmp-profile)# match identity address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128	Matches an identity from a remote peer in an ISAKMP profile.

Configuring IPv6 IPsec VTI

This task describes how to configure and enable IPv6 IPsec virtual tunnel mode for IPv6.

Prerequisites

Use the **ipv6 unicast-routing** command to enable IPv6 unicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface tunnel** *tunnel-number*
5. **ipv6 address** *ipv6-address/prefix*
6. **ipv6 enable**

7. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
8. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
9. **tunnel mode** {*aurp* | *cayman* | *dvmrp* | *eon* | *gre* | *gre multipoint* | *gre ipv6* | *ipip* | *decapsulate-any* | *ipsec ipv4* | *iptalk* | *ipv6* | *ipsec ipv6* | *mpls* | *nos* | *rbscp*}
10. **tunnel protection ipsec profile** *name* [*shared*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ipv6 unicast-routing Example: Router(config)# ipv6 unicast-routing	Enables IPv6 unicast routing. You only need to enable IPv6 unicast routing once, not matter how many interface tunnels you want to configure.
Step 4	interface tunnel <i>tunnel-number</i> Example: Router(config)# interface tunnel 0	Specifies a tunnel interface and number, and enters interface configuration mode.
Step 5	ipv6 address <i>ipv6-address/prefix</i> Example: Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64	Provides an IPv6 address to this tunnel interface, so that IPv6 traffic can be routed to this tunnel.
Step 6	ipv6 enable Example: Router(config-if)# ipv6 enable	Enables IPv6 on this tunnel interface.
Step 7	tunnel source { <i>ip-address</i> <i>ipv6-address</i> <i>interface-type interface-number</i> } Example: Router(config-if)# tunnel source ethernet0	Sets the source address for a tunnel interface.
Step 8	tunnel destination { <i>host-name</i> <i>ip-address</i> <i>ipv6-address</i> } Example: Router(config-if)# tunnel destination 2001:0DB8:1111:2222::1	Specifies the destination for a tunnel interface.

	Command or Action	Purpose
Step 9	<pre>tunnel mode {aurp cayman dvmrp eon gre gre multipoint gre ipv6 ipip [decapsulate-any] ipsec ipv4 iptalk ipv6 ipsec ipv6 mpls nos rbscp}</pre> <p>Example: Router(config-if)# tunnel mode ipsec ipv6</p>	Sets the encapsulation mode for the tunnel interface. For IPsec, only the ipsec ipv6 keywords are supported.
Step 10	<pre>tunnel protection ipsec profile name [shared]</pre> <p>Example: Router(config-if)# tunnel protection ipsec profile profile1</p>	Associates a tunnel interface with an IPsec profile. IPv6 does not support the shared keyword.

Verifying IPsec Tunnel Mode Configuration

This optional task describes how to display information to verify IPsec tunnel mode configuration. Use the following commands as needed to verify configuration and operation.

SUMMARY STEPS

1. **show adjacency** [**summary** [*interface-type interface-number*]] | [*prefix*] [*interface interface-number*] [**connectionid id**] [**link {ipv4 | ipv6 | mpls}**] [**detail**]
2. **show crypto engine** {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** | **dropped-packet** | **show**] | **qos**}
3. **show crypto ipsec sa** [**ipv6**] [*interface-type interface-number*] [**detailed**]
4. **show crypto isakmp peer** [**config** | **detail**]
5. **show crypto isakmp policy**
6. **show crypto isakmp profile**
7. **show crypto map** [**interface interface** | **tag map-name**]
8. **show crypto session** [**detail**] | [**local ip-address** [**port local-port**]] | [**remote ip-address** [**port remote-port**]] | [**detail**] | [**fvrf vrf-name**] | [**ivrf vrf-name**]
9. **show crypto socket**
10. **show ipv6 access-list** [*access-list-name*]
11. **show ipv6 cef** [**vrf**] [*ipv6-prefix/prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]
12. **show interface type number stats**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>show adjacency [summary [interface-type interface-number]] [prefix] [interface interface-number] [connectionid id] [link {ipv4 ipv6 mpls}] [detail]</pre> <p>Example: Router# show adjacency detail</p>	Displays information about the CEF adjacency table or the hardware Layer 3-switching adjacency table.
Step 2	<pre>show crypto engine {accelerator brief configuration connections [active dh dropped-packet show] qos}</pre> <p>Example: Router# show crypto engine connection active</p>	Displays a summary of the configuration information for the crypto engines.
Step 3	<pre>show crypto ipsec sa [ipv6] [interface-type interface-number] [detailed]</pre> <p>Example: Router# show crypto ipsec sa ipv6</p>	Displays the settings used by current SAs in IPv6.
Step 4	<pre>show crypto isakmp peer [config detail]</pre> <p>Example: Router# show crypto isakmp peer detail</p>	Displays peer descriptions.
Step 5	<pre>show crypto isakmp policy</pre> <p>Example: Router# show crypto isakmp policy</p>	Displays the parameters for each IKE policy.
Step 6	<pre>show crypto map [interface interface tag map-name]</pre> <p>Example: Router# show crypto map</p>	<p>Displays the crypto map configuration.</p> <p>The crypto maps shown in this command output are dynamically generated. The user does not have to configure crypto maps.</p>
Step 7	<pre>show crypto session [detail] [local ip-address [port local-port] [remote ip-address [port remote-port]] [detail]] [fvfr vrf-name] [ivrf vrf-name]</pre> <p>Example: Router# show crypto session</p>	<p>Displays status information for active crypto sessions.</p> <p>IPv6 does not support the fvfr or ivrf keywords or the <i>vrf-name</i> argument.</p>
Step 8	<pre>show crypto socket</pre> <p>Example: Router# show crypto socket</p>	Lists crypto sockets.

	Command or Action	Purpose
Step 9	<code>show ipv6 access-list [access-list-name]</code> Example: Router# show ipv6 access-list	Displays the contents of all current IPv6 access lists.
Step 10	<code>show ipv6 cef [ipv6-prefix/prefix-length] [interface-type interface-number] [longer-prefixes similar-prefixes detail internal platform epoch source]</code> Example: Router# show ipv6 cef	Displays entries in the IPv6 Forwarding Information Base (FIB).
Step 11	<code>show interface type number stats</code> Example: Router# show interface fddi 3/0/0 stats	Displays numbers of packets that were process switched, fast switched, and distributed switched.

Troubleshooting IPsec for IPv6 Configuration and Operation


This optional task explains how to display information to troubleshoot the configuration and operation of IPv6 IPsec. Use the following commands only as needed to verify configuration and operation.

SUMMARY STEPS

1. `enable`
2. `debug crypto ipsec [error]`
3. `debug crypto engine packet [detail] [error]`
4. `debug crypto isakmp [error]`
5. `debug crypto socket [error]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	<code>debug crypto ipsec</code> Example: Router# <code>debug crypto ipsec</code>	Displays IPsec network events.
Step 3	<code>debug crypto engine packet [detail]</code> Example: Router# <code>debug crypto engine packet</code>	Displays the contents of IPv6 packets.  Caution Using this command could flood the system and increase CPU if several packets are being encrypted.

Examples

This section provides the following output examples:

- [Sample Output for the show crypto ipsec sa Command, page 15](#)
- [Sample Output for the show crypto isakmp peer Command, page 16](#)
- [Sample Output for the show crypto isakmp profile Command, page 16](#)
- [Sample Output for the show crypto isakmp sa Command, page 17](#)
- [Sample Output for the show crypto map Command, page 17](#)
- [Sample Output for the show crypto session Command, page 17](#)

Sample Output for the show crypto ipsec sa Command

The following is sample output from the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::A8BB:CCFF:FE01:9002

  protected vrf: (none)
  local ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (::/0/0/0)
  current_peer 3FFE:2002::A8BB:CCFF:FE01:2C02 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 133, #pkts encrypt: 133, #pkts digest: 133
    #pkts decaps: 133, #pkts decrypt: 133, #pkts verify: 133
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 60, #recv errors 0

  local crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:9002,
  remote crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:2C02
  path mtu 1514, ip mtu 1514
  current outbound spi: 0x28551D9A(676666778)

inbound esp sas:
  spi: 0x2104850C(553944332)
    transform: esp-des ,
    in use settings ={Tunnel, }
    conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4397507/148)
```

```

IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
spi: 0x967698CB(2524354763)
transform: ah-sha-hmac ,
in use settings ={Tunnel, }
conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4397507/147)
replay detection support: Y
Status: ACTIVE

inbound pcp sas:

outbound esp sas:
spi: 0x28551D9A(676666778)
transform: esp-des ,
in use settings ={Tunnel, }
conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4397508/147)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
spi: 0xA83E05B5(2822636981)
transform: ah-sha-hmac ,
in use settings ={Tunnel, }
conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4397508/147)
replay detection support: Y
Status: ACTIVE

outbound pcp sas:

```

Sample Output for the show crypto isakmp peer Command

The following sample output shows peer descriptions on an IPv6 router:

```

Router# show crypto isakmp peer detail

Peer: 2001:0DB8:0:1::1 Port: 500 Local: 2001:0DB8:0:2::1
Phase1 id: 2001:0DB8:0:1::1
flags:
NAS Port: 0 (Normal)
IKE SAs: 1 IPsec SA bundles: 1
last_locker: 0x141A188, last_last_locker: 0x0
last_unlocker: 0x0, last_last_unlocker: 0x0

```

Sample Output for the show crypto isakmp profile Command

The following sample output shows the ISAKMP profiles that are defined on an IPv6 router.

```

Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>

```


Sample Output for the show crypto isakmp sa Command

The following sample output shows the SAs of an active IPv6 device. The IPv4 device is inactive:

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
src: 3FFE:2002::A8BB:CCFF:FE01:9002
conn-id: 1001 I-VRF: Status: ACTIVE Encr: des Hash: sha Auth:
psk
DH: 1 Lifetime: 23:45:00 Cap: D Engine-id:Conn-id = SW:1

dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
src: 3FFE:2002::A8BB:CCFF:FE01:9002
conn-id: 1002 I-VRF: Status: ACTIVE Encr: des Hash: sha Auth: psk
DH: 1 Lifetime: 23:45:01 Cap: D Engine-id:Conn-id = SW:2
```

Sample Output for the show crypto map Command

The following sample output shows the dynamically generated crypto maps of an active IPv6 device:

```
Router# show crypto map

Crypto Map "Tunnell-head-0" 65536 ipsec-isakmp
  Profile name: profile0
  Security association lifetime: 4608000 kilobytes/300 seconds
  PFS (Y/N): N
  Transform sets={
    ts,
  }

Crypto Map "Tunnell-head-0" 65537
  Map is a PROFILE INSTANCE.
  Peer = 2001:1::2

IPv6 access list Tunnell-head-0-ACL (crypto)
  permit ipv6 any any (61445999 matches) sequence 1
  Current peer: 2001:1::2
  Security association lifetime: 4608000 kilobytes/300 seconds
  PFS (Y/N): N
  Transform sets={
    ts,
  }
  Interfaces using crypto map Tunnell-head-0:
  Tunnell
```

Sample Output for the show crypto session Command

The following output from the show crypto session information provides details on currently active crypto sessions:

```
Router# show crypto session detail
```

```

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection K - Keepalives, N -
NAT-traversal, X - IKE Extended Authentication

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 2001:1::1 port 500 fvrf: (none) ivrf: (none)
      Phasel_id: 2001:1::1
      Desc: (none)
      IKE SA: local 2001:1::2/500
              remote 2001:1::1/500 Active
              Capabilities:(none) connid:14001 lifetime:00:04:32
IPSEC FLOW: permit ipv6 ::/0 ::/0
      Active SAs: 4, origin: crypto map
      Inbound:  #pkts dec'ed 42641 drop 0 life (KB/Sec) 4534375/72
      Outbound: #pkts enc'ed 6734980 drop 0 life (KB/Sec) 2392402/72

```

Configuration Examples for IPsec for IPv6 Security

This section provides the following configuration example:

- [Configuring a VTI for Site-to-Site IPv6 IPsec Protection: Example, page 18](#)

Configuring a VTI for Site-to-Site IPv6 IPsec Protection: Example

The following example shows configuration for a single IPv6 IPsec tunnel:

```

crypto isakmp policy 1
  authentication pre-share
!
crypto isakmp key myPreshareKey0 address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128
crypto isakmp keepalive 30 30
!
crypto ipsec transform-set 3des ah-sha-hmac esp-3des
!
crypto ipsec profile profile0
  set transform-set 3des
!
ipv6 cef
!
interface Tunnel0
  ipv6 address 3FFE:1001::/64 eui-64
  ipv6 enable
  ipv6 cef
  tunnel source Ethernet2/0
  tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile profile0

```

Additional References

The following sections provide references related to the Implementing IPsec in IPv6 Security feature.

Related Documents

Related Topic	Document Title
OSPF for IPv6 authentication support with IPsec	<i>Implementing OSPF for IPv6</i>
IPsec VTI information	<i>IPsec Virtual Tunnel Interface</i> , Release 12.3(14)T
IPv6 supported feature list	<i>Start Here: Cisco IOS Software Release Specifics for IPv6 Features</i>
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IPv6 Command Reference</i>
IPv4 security configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4
IPv4 security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.4
IPv4 configuration and command reference information	Cisco IOS Configuration Guides and Command References, Release 12.4

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2401	<i>Security Architecture for the Internet Protocol</i>
RFC 2402	<i>IP Authentication Header</i>
RFC 2404	<i>The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header</i>
RFC 2406	<i>IP Encapsulating Security Payload (ESP)</i>
RFC 2407	<i>The Internet Security Domain of Interpretation for ISAKMP</i>
RFC 2408	<i>Internet Security Association and Key Management Protocol (ISAKMP)</i>
RFC 2409	<i>Internet Key Exchange (IKE)</i>
RFC 2460	<i>Internet Protocol, Version 6 (IPv6) Specification</i>
RFC 2474	<i>Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</i>
RFC 3576	<i>Change of Authorization</i>

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Implementing IPsec in IPv6 Security

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(4)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see “Start Here: Cisco IOS Software Release Specifies for IPv6 Features.”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Implementing IPsec in IPv6 Security

Feature Name	Releases	Feature Information
IPv6 IPsec to Authenticate Open Shortest Path First for IPv6 (OSPFv3)	12.3(4)T, 12.4, 12.4(2)T	OSPF for IPv6 uses the IP Security (IPsec) secure socket application program interface (API) to add authentication to OSPF for IPv6 packets. This API has been extended to provide support for IPv6. The following sections provide information about this feature: <ul style="list-style-type: none"> • OSPF for IPv6 Authentication Support with IPsec, page 2 • How to Implement IPsec for IPv6 Security, page 4
IPv6 IPsec VPN	12.4(4)T	The following sections provide information about this feature: <ul style="list-style-type: none"> • Information About Implementing IPsec for IPv6 Security, page 2 • How to Implement IPsec for IPv6 Security, page 4

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Table 2 Minimum Required Cisco IOS Release

Feature	Minimum Required Cisco IOS Release by Release Train
IPv6 IPsec to Authenticate Open Shortest Path First for IPv6 (OSPFv3)	The following sections provide information about this feature:
	12.4(4)T

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.