



# IPSec Passive Mode

---

## Feature History

Release	Modification
12.2(13)T	This feature was introduced.

This feature module describes the IPSec Passive Mode feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 9](#)

## Feature Overview

The IPSec Passive Mode feature allows users to configure an intermediate mode—IP Security (IPSec) passive mode—that enables routers within an existing network to accept both encrypted and unencrypted data. The routers will attempt to negotiate an encrypted session when sending data, but they will send the data in unencrypted form as necessary.

IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec. Users no longer have wait for all routers to deploy IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.



### Note

---

Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

---

## How IPSec Passive Mode Works

After a user enables IPSec passive mode, the following behaviors occur:

- If a packet is routed through an interface that is configured to encrypt the packet, and an active security association (SA) that is used to send the packet is not available, one of the following actions occur:
  - If it has not been 10 seconds since the packet was initially sent, the packet is dropped and an attempt to establish an SA using the Internet Key Exchange (IKE) occurs as normal.
  - If it has been at 10 seconds since the packet was initially sent, the packet is routed in the clear (unencrypted), and a rate-limited warning message is sent to the error log.
  - If the configured number of seconds since the last attempt to establish an SA via IKE has been reached, the packet is routed in the clear, and an attempt to establish a connection using IKE is tried again.




---

**Note** If an SA is established for a packet type, the timer is reset.

---

- If a packet comes through an interface that is configured to decrypt the packet and the packet is in the clear, the packet is accepted and a rate-limited error message is sent. This behavior occurs even if there is an SA that could have encrypted the packet because the packet may have been routed through a redundant peer that has not yet been configured for IPSec.

## Warning Messages

IPSec passive mode behavior produces the following logged warning messages:

- “Security warning: crypto ipsec optional is configured”  
This warning message, which is sent every 10 minutes, is displayed to remind the user that passive mode is enabled, so security is optional.
- “Unencrypted traffic is sent to 10.0.0.1 because crypto optional is configured”
- “Unencrypted traffic is received from 10.0.0.1 because crypto optional is configured”

These messages, which are sent once every minute, are rate-limited warning messages that are displayed when plain (unencrypted) text is sent or received.




---

**Note** The direction indication of the IP address is from one of the packets that is sent or accepted during the interval. The IP address is provided to help the administrator find nodes that still have to be upgraded.

---

## Benefits

### Easy IPSec Deployment

IPSec passive mode enables an existing network to easily implement IPSec because the routers within the network will accept encrypted and unencrypted data. Thus, the downtime required to enhance your existing network is significantly reduced because users no longer have to wait for all routers within the network to deploy IPSec.

### IPSec Passive Mode Compatibility

This feature is compatible with all hardware encryption cards.

## Related Documents

- The part “IP Security and Encryption” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The part “IP Security and Encryption” in the *Cisco IOS Security Command Reference*, Release 12.2

## Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

# Supported Standards, MIBs, and RFCs

## Standards

None

## MIBs

None

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

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

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

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

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

None

## Prerequisites

Before enabling IPSec passive mode, IPSec must be implemented on your system. (For information on completing this task, see the chapter “Configuring IPSec Network Security” in the *Cisco IOS Security Configuration Guide*, Release 12.2.)

## Configuration Tasks

See the following sections for configuration tasks for the IPSec Passive Mode feature. Each task in the list is identified as either required or optional.

- [Configuring IPSec Passive Mode](#) (required)
- [Verifying IPSec Passive Mode](#) (optional)

## Configuring IPSec Passive Mode

To enable IPSec Passive mode, use the following global configuration commands:

Command	Purpose
Router(config)# <b>crypto ipsec optional</b>	Enables IPSec passive mode on a router.
Router(config)# <b>crypto ipsec optional retry seconds</b>	Allows users to adjust the time that packets can be sent in the clear (unencrypted) before another attempt is made to establish an encrypted IPSec connection.

## Verifying IPSec Passive Mode

To verify the passive mode status, use the following privilege EXEC command:

Command	Purpose
Router# <b>show crypto optional</b>	Displays the passive mode status.  If passive mode is not enabled, the output will display the following text: "Passive mode disabled." If passive mode is enabled, the output will display the following text: "Passive mode enabled. IPSec is currently insecure." The output will also list the various destinations you are currently sending packets in the clear because passive mode is enabled.

## Configuration Examples

This section provides the following configuration example:

- [IPSec Passive Mode Example](#)

### IPSec Passive Mode Example

The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
  ip address 209.165.202.147 255.255.255.224
  crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

# Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [crypto ipsec optional](#)
- [crypto ipsec optional retry](#)

# crypto ipsec optional

To enable IP Security (IPSec) passive mode, use the **crypto ipsec optional** command in global configuration mode. To disable IPSec passive mode, use the **no** form of this command.

**crypto ipsec optional**

**no crypto ipsec optional**

**Syntax Description** This command has no arguments or keywords.

**Defaults** IPSec passive mode is not enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

**Usage Guidelines** Use the **crypto ipsec optional** command to implement an intermediate mode (IPSec passive mode) that allows a router to accept unencrypted and encrypted data. IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.

After this feature is disabled, all active connections that are sending unencrypted packets are cleared, and a message that reminds the user to enter the **write memory** command is sent.



**Note**

Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

**Examples** The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
  ip address 209.165.202.147 255.255.255.224
  crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

# crypto ipsec optional retry

To adjust the amount of time that a packet can be routed in the clear (unencrypted), use the **crypto ipsec optional retry** command in global configuration mode. To return to the default setting (5 minutes), use the **no** form of this command.

**crypto ipsec optional retry** *seconds*

**no crypto ipsec optional retry** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time a connection can exist before another attempt is made to establish an encrypted IP Security (IPSec) session. The default value is 5 minutes.
---------------------------	----------------	---

<b>Defaults</b>	5 minutes
-----------------	-----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.

<b>Usage Guidelines</b>	You must enable the <b>crypto ipsec optional</b> command, which enables IPSec passive mode, before you can use this command.
-------------------------	--

<b>Examples</b>	The following example shows how to enable IPSec passive mode:
-----------------	---

```
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
crypto ipsec optional
crypto ipsec optional retry 60
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">crypto ipsec optional</a>	Enables IPSec passive mode.

# Glossary

**IKE**—Internet Key Exchange. Hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. Although IKE can be used with other protocols, its initial implementation is with IPSec. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations (SAs).

**IPSec**—IP Security. Framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides 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.

**SA**—security association. Description on how two or more entities will utilize security services to communicate securely. For example, an IPSec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPSec connection.

Both IPSec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPSec SA is established either by IKE or by manual user configuration.

