



# IP Security VPN Monitoring

---

**First Published: November 3, 2003**

**Last Updated: March 29, 2011**

The IP Security VPN Monitoring feature provides the following Virtual Private Network (VPN) session monitoring enhancements to troubleshoot and monitor the end-user interface:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for IP Security VPN Monitoring” section on page 8](#).

Use Cisco Feature Navigator to find information about platform support and Cisco 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 IP Security VPN Monitoring, page 2](#)
- [Restrictions for IP Security VPN Monitoring, page 2](#)
- [Information About IPSec VPN Monitoring, page 2](#)
- [How to Configure IP Security VPN Monitoring, page 4](#)
- [Configuration Examples for IP Security VPN Monitoring, page 6](#)



---

**Americas Headquarters:**

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

- [Additional References, page 7](#)
- [Feature Information for IP Security VPN Monitoring, page 8](#)

## Prerequisites for IP Security VPN Monitoring

- You should be familiar with IPSec and encryption.
- Your router must support IPSec, and before using the IP Security VPN Monitoring feature, you must have configured IPSec on your router.

## Restrictions for IP Security VPN Monitoring

- You must be running Cisco IOS k8 or k9 crypto images on your router.

## Information About IPSec VPN Monitoring

To troubleshoot the IPSec VPN and monitor the end-user interface, you should understand the following concepts:

- [Background: Crypto Sessions, page 2](#)
- [Per-IKE Peer Description, page 2](#)
- [Summary Listing of Crypto Session Status, page 3](#)
- [Syslog Notification for Crypto Session Up or Down Status, page 3](#)
- [IKE and IPSec Security Exchange Clear Command, page 3](#)

## Background: Crypto Sessions

A crypto session is a set of IPSec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPSec security associations (for data traffic—one per each direction). There may be duplicated IKE security associations (SAs) and IPSec SAs or duplicated IKE SAs or IPSec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

## Per-IKE Peer Description

The Per-IKE Peer Description function allows you to enter a description of your choosing for an IKE peer. (Before Cisco IOS Release 12.3(4)T, you could use only the IP address or fully qualified domain name [FQDN] to identify the peer; there was no way to configure a description string.) The unique peer description, which can include up to 80 characters, can be used whenever you are referencing that particular IKE peer. To add the peer description, use the **description** command.

**Note**

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

The primary application of this description field is for monitoring purposes (for example, when using **show** commands or for logging [syslog messages]). The description field is purely informational (for example, it cannot act as a substitute for the peer address or FQDN when defining crypto maps).

## Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

## Syslog Notification for Crypto Session Up or Down Status

The Syslog Notification for Crypto Session Up or Down Status function provides syslog notification every time the crypto session comes up or goes down.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20  
Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10  
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

## IKE and IPsec Security Exchange Clear Command

In previous IOS versions, there was no single command to clear both IKE and IPsec connections (that is, SAs). Instead, you had to use the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The new **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you use the **clear crypto session** command, all IPSec SAs and IKE SAs that are in the router will be deleted.

## How to Configure IP Security VPN Monitoring

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

- [Adding the Description of an IKE Peer, page 4](#) (optional)
- [Verifying Peer Descriptions, page 5](#) (optional)
- [Clearing a Crypto Session, page 6](#) (optional)

### Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPSec VPN session, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer {ip-address ip-address}**
4. **description**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>crypto isakmp peer</b> {ip-address ip-address}  <b>Example:</b> Router (config)# crypto isakmp peer address 10.2.2.9	Enables an IPSec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode.
Step 4	<b>description</b>  <b>Example:</b> Router (config-isakmp-peer)# description connection from site A	Adds a description for an IKE peer.

## Verifying Peer Descriptions

To verify peer descriptions, use the **show crypto isakmp peer** command.

### SUMMARY STEPS

1. **enable**
2. **show crypto isakmp peer**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show crypto isakmp peer</b>  <b>Example:</b> Router# show crypto isakmp peer	Displays peer descriptions.

## Examples

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer

Peer: 10.2.2.9 Port: 500
Description: connection from site A
flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection from site A Id: ezvpn
```

## Clearing a Crypto Session

To clear a crypto session, use the **clear crypto session** command from the router command line. No configuration statements are required in the configuration file to use this command.

### SUMMARY STEPS

1. **enable**
2. **clear crypto session**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>clear crypto session</b>  <b>Example:</b> Router# clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).

## Configuration Examples for IP Security VPN Monitoring

This section provides the following configuration example:

- [show crypto session Command Output: Examples, page 6](#)

### show crypto session Command Output: Examples

The following is sample output for the **show crypto session** output without the **detail** keyword:

```
Router# show crypto session

Crypto session current status

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
    IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
    IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
    Active SAs: 2, origin: crypto map
```

The following is sample output using the **show crypto session command and the detail** keyword:

```
Router# show crypto session detail

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
    Desc: this is my peer at 10.1.1.3:500 Green
```

```

Phase1_id: 10.1.1.3
IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
  Capabilities:(none) connid:3 lifetime:22:03:24
IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
  Active SAs: 0, origin: crypto map
  Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
  Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
  Active SAs: 4, origin: crypto map
  Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
  Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949

```

## Additional References

### Related Documents

Related Topic	Document Title
IP security, encryption, and IKE	<ul style="list-style-type: none"> <li><a href="#">Configuring Internet Key Exchange for IPsec VPNs</a></li> <li><a href="#">Configuring Security for VPNs with IPsec</a></li> </ul>
Security commands	<a href="#">Cisco IOS Security Command Reference</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for IP Security VPN Monitoring

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1** Feature Information for IP Security VPN Monitoring

Feature Name	Releases	Feature Information
IP Security VPN Monitoring	12.3(4)T	<p>The IP Security VPN Monitoring feature provides the following Virtual Private Network (VPN) session monitoring enhancements to troubleshoot and monitor the end-user interface:</p> <ul style="list-style-type: none"> <li>• Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file</li> <li>• Summary listing of crypto session status</li> <li>• Syslog notification for crypto session up or down status</li> <li>• Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)</li> </ul> <p>This feature was introduced in Cisco IOS Release 12.3(4)T.</p> <p>The following commands were introduced or modified:  <b>clear crypto session, description (isakmp peer), show crypto isakmp peers, show crypto session.</b></p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

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

© 2003–2011 Cisco Systems, Inc. All rights reserved.