# ıllıılı
# CISCO ™

**IPsec Management Configuration Guide
Cisco IOS Release 12.2SX**

# C O N T E N T S

# IP Security VPN Monitoring

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 Table at the end of this document.

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

## 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

## 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

## 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** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **crypto isakmp peer** {**ip-address***ip-address* }<br><br>**Example:**<br><br>`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** | **description**<br><br>**Example:**<br><br>`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** | **enable** | Enables privileged EXEC mode. |
|  | | • Enter your password if prompted. |
|  | **Example:** | |
|  | Router> enable | |
| **Step 2** | **show crypto isakmp peer** | Displays peer descriptions. |
|  | **Example:** | |
|  | Router# show crypto isakmp peer | |

### 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
```

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** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **clear crypto session**<br><br>**Example:**<br><br>`Router# clear crypto session` | Deletes crypto sessions (IPSec and IKE SAs). |

# Configuration Examples for IP Security VPN Monitoring

## 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 | • Configuring Internet Key Exchange for IPsec VPNs<br>• Configuring Security for VPNs with IPsec |
| Security commands | *Cisco IOS Security Command Reference* |

**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:<br>http://www.cisco.com/go/mibs |

**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 |

# Feature Information for IP Security VPN Monitoring

The following table provides release information about the feature or features described in this module. This table 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.

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

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

| Feature Name | Releases | Feature Information |
| --- | --- | --- |
| IP Security VPN Monitoring | 12.3(4)T | The IP Security VPN Monitoring feature provides the following Virtual Private Network (VPN) session monitoring enhancements to troubleshoot and monitor the end-user interface:<br><br>• Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file<br>• Summary listing of crypto session status<br>• Syslog notification for crypto session up or down status<br>• Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)<br><br>This feature was introduced in Cisco IOS Release 12.3(4)T.<br><br>The following commands were introduced or modified: **clear crypto session, description (isakmp peer), show crypto isakmp peers, show crypto session .** |

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.

# IPsec VPN Accounting

The IPsec VPN Accounting feature allows a session to be accounted by indicating when the session starts and stops. A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted. Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server through standard RADIUS attributes and vendor-specific attributes (VSAs).

# 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 Table at the end of this document.

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

# Prerequisites for IPsec VPN Accounting

- You should understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting.
- You should know how to configure IPsec accounting.

# Information About IPsec VPN Accounting

# RADIUS Accounting

For many large networks, it is required that user activity be recorded for auditing purposes. The method that is used most is RADIUS accounting.

RADIUS accounting allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information is passed to the RADIUS server through RADIUS attributes and VSAs.

## RADIUS Start Accounting

The RADIUS Start packet contains many attributes that generally identify who is requesting the service and of what the property of that service consists. The table below represents the attributes required for the start.

*Table 2      RADIUS Accounting Start Packet Attributes*

| RADIUS Attributes Value | Attribute | Description |
| --- | --- | --- |
| 1 | user-name | Username used in extended authentication (XAUTH).The username may be NULL when XAUTH is not used. |
| 4 | nas-ip-address | Identifying IP address of the network access server (NAS) that serves the user. It should be unique to the NAS within the scope of the RADIUS server. |
| 5 | nas-port | Physical port number of the NAS that serves the user. |
| 8 | framed-ip-address | Private address allocated for the IP Security (IPsec) session. |
| 40 | acct-status-type | Status type. This attribute indicates whether this accounting request marks the beginning (start), the end (stop), or an update of the session. |
| 41 | acct-delay-time | Number of seconds the client has been trying to send a particular record. |

| RADIUS Attributes Value | Attribute | Description |
|---|---|---|
| 44 | acct-session-id | Unique accounting identifier that makes it easy to match start and stop records in a log file. |
| 26 | vrf-id | String that represents the name of the Virtual Route Forwarder (VRF). |
| 26 | isakmp-initiator-ip | Endpoint IP address of the remote Internet Key Exchange (IKE) initiator (V4). |
| 26 | isakmp-group-id | Name of the VPN group profile used for accounting. |
| 26 | isakmp-phase1-id | Phase 1 identification (ID) used by IKE (for example, domain name [DN], fully qualified domain name [FQDN], IP address) to help identify the session initiator. |

## RADIUS Stop Accounting

The RADIUS Stop packet contains many attributes that identify the usage of the session. Table 2 represents the additional attributes required for the RADIUS stop packet. It is possible that only the stop packet is sent without the start if configured to do so. If only the stop packet is sent, this allows an easy way to reduce the number of records going to the AAA server.

*Table 3*        *RADIUS Accounting Stop Packet Attributes*

| RADIUS Attributes Value | Attribute | Description |
|---|---|---|
| 42 | acct-input-octets | Number of octets that have been received from the Unity client over the course of the service that is being provided. |
| 43 | acct-output-octets | Number of octets that have been sent to the Unity client in the course of delivering this service. |
| 46 | acct-session-time | Length of time (in seconds) that the Unity client has received service. |

| RADIUS Attributes Value | Attribute | Description |
|---|---|---|
| 47 | acct-input-packets | Quantity of packets that have been received from the Unity client in the course of delivering this service. |
| 48 | acct-output-packets | Quantity of packets that have been sent to the Unity client in the course of delivering this service. |
| 49 | acct-terminate-cause | For future use. |
| 52 | acct-input-gigawords | How many times the Acct-Input-Octets counter has wrapped around the 232 (2 to the 32nd power) over the course of this service. |
| 52 | acct-output-gigawords | How many times the Acct-Input-Octets counter has wrapped around the 232 (2 to the 32nd power) over the course of this service. |

## RADIUS Update Accounting

RADIUS accounting updates are supported. Packet and octet counts are shown in the updates.

# IKE and IPsec Subsystem Interaction

## Accounting Start

If IPsec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

The following is an account start record that was generated on a router and that is to be sent to the AAA server that is defined:

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4,
len 220
*Aug 23 04:06:20.131: RADIUS:  authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19
FB 3F
*Aug 23 04:06:20.135: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  31
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   25  "isakmp-group-id=cclient"
```

```
*Aug 23 04:06:20.135: RADIUS:  Framed-IP-Address    [8]   6   10.13.13.1
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco         [26]  20
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair         [1]   14  "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco         [26]  35
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair         [1]   29  "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco         [26]  36
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair         [1]   30  "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS:  User-Name            [1]   13  "joe@cclient"
*Aug 23 04:06:20.135: RADIUS:  Acct-Status-Type     [40]  6   Start                  [1]
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco         [26]  25
*Aug 23 04:06:20.135: RADIUS:   cisco-nas-port      [2]   19  "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS:  NAS-Port             [5]   6   0
*Aug 23 04:06:20.135: RADIUS:  NAS-IP-Address       [4]   6   10.1.1.147
*Aug 23 04:06:20.135: RADIUS:  Acct-Delay-Time      [41]  6   0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-
response, len 20
*Aug 23 04:06:20.139: RADIUS:  authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

## Accounting Stop

An accounting stop packet is generated when there are no more flows (IPsec SA pairs) with the remote peer.

The accounting stop records contain the following information:

- Packets out
- Packets in
- Octets out
- Gigawords in
- Gigawords out

Below is an account start record that was generated on a router. The account start record is to be sent to the AAA server that is defined.

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS:  authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco         [26]  20
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair         [1]   14  "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco         [26]  35
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair         [1]   29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco         [26]  36
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair         [1]   30  "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Time    [46]  6   709
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Octets    [42]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Octets   [43]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Packets   [47]  6   1004
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Packets  [48]  6   1004
*Apr 23 04:20:16.519: RADIUS:  Acct-Input-Giga-Word [52]  6   0
*Apr 23 04:20:16.519: RADIUS:  Acct-Output-Giga-Wor [53]  6
0
*Aug 23 04:20:16.519: RADIUS:  Acct-Terminate-Cause [49]  6   none                   [0]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco         [26]  32
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair         [1]   26  "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS:  Acct-Status-Type     [40]  6   Stop                   [2]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco         [26]  25
*Aug 23 04:20:16.519: RADIUS:   cisco-nas-port      [2]   19  "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS:  NAS-Port             [5]   6   0
*Aug 23 04:20:16.519: RADIUS:  NAS-IP-Address       [4]   6   100.1.1.147
*Aug 23 04:20:16.519: RADIUS:  Acct-Delay-Time      [41]  6   0
```

```
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646, Accounting-
response, len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

## Accounting Updates

If accounting updates are enabled, accounting updates are sent while a session is "up." The update interval can be configured. To enable the accounting updates, use the **aaa accounting update** command.

The following is an accounting update record that is being sent from the router:

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id    [44]  10   "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26]  20
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair      [1]   14   "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26]  35
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair      [1]   29   "isakmp-initator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26]  36
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair      [1]   30   "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time  [46]  6    109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets  [42]  6    608
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets [43]  6    608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets [47]  6    4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48] 6    4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type   [40]  6    Watchdog                [3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco      [26]  25
*Aug 23 21:46:05.263: RADIUS:   cisco-nas-port    [2]   19   "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port           [5]   6    0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address     [4]   6    100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time    [41]  6    0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646, Accounting-
response, len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

# How to Configure IPsec VPN Accounting

## Configuring IPsec VPN Accounting

To enable IPsec VPN Accounting, you need to perform the following required task:

Before configuring IPsec VPN accounting, you must first configure IPsec.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name method*
5. **aaa authorization network** *list-name method*
6. **aaa accounting network list-name start-stop [broadcast] group** *group-name*
7. **aaa session-id common**
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrf*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address [ initiate | respond ]**
14. **accounting** *list-name*
15. **exit**
16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route [ remote-peer ]**
20. **exit**
21. **crypto map** *map-name* ipsec-isakmp dynamic *dynamic-template-name*
22. **radius-server hos** t *ip-address* [**auth-port***port-number]*[**acct-port***port-number* ]
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *type slot /port*
26. **crypto map** *map-name*

## DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>Router# configure terminal | Enters global configuration mode. |
| Step 3 | **aaa new-model**<br><br>**Example:**<br><br>Router (config)# aaa new-model | Enables periodic interim accounting records to be sent to the accounting server. |
| Step 4 | **aaa authentication login** *list-name method*<br><br>**Example:**<br><br>Router (config)# aaa authentication login cisco-client group radius | Enforces authentication, authorization, and accounting (AAA) authentication for extended authorization (XAUTH) through RADIUS or local. |
| Step 5 | **aaa authorization network** *list-name method*<br><br>**Example:**<br><br>Router (config)# aaa authorization network cisco-client group radius | Sets AAA authorization parameters on the remote client from RADIUS or local. |
| Step 6 | **aaa accounting network list-name start-stop [broadcast] group** *group-name*<br><br>**Example:**<br><br>Router (config)# aaa accounting network acc start-stop broadcast group radius | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS +. |
| Step 7 | **aaa session-id common**<br><br>**Example:**<br><br>Router (config)# aaa session-id common | Specifies whether the same session ID is used for each AAA accounting service type within a call or whether a different session ID is assigned to each accounting service type. |
| Step 8 | **crypto isakmp profile** *profile-name*<br><br>**Example:**<br><br>Route (config)# crypto isakmp profile cisco | Audits IP security (IPsec) user sessions and enters isakmp-profile submode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 9 | **vrf** *ivrf*<br><br>**Example:**<br><br>`Router (conf-isa-prof)# vrf cisco` | Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name. |
| Step 10 | **match identity group** *group-name*<br><br>**Example:**<br><br>`Router(conf-isa-prof)# match identity group cisco` | Matches an identity from a peer in an ISAKMP profile. |
| Step 11 | **client authentication list** *list-name*<br><br>**Example:**<br><br>`Router(conf-isa-prof)# client authentication list cisco` | Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile. |
| Step 12 | **isakmp authorization list** *list-name*<br><br>**Example:**<br><br>`Router(conf-isa-prof)#` **isakmp authorization list cisco-client** | Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer through mode configuration (MODECFG). |
| Step 13 | **client configuration address [ initiate | respond ]**<br><br>**Example:**<br><br>`Router(conf-isa-prof)# client configuration address respond` | Configures IKE mode configuration (MODECFG) in the ISAKMP profile. |
| Step 14 | **accounting** *list-name*<br><br>**Example:**<br><br>`Router(conf-isa-prof)# accounting acc` | Enables AAA accounting services for all peers that connect through this ISAKMP profile. |
| Step 15 | **exit**<br><br>**Example:**<br><br>`Router(conf-isa-prof)# exit` | Exits isakmp-profile submode. |

| Command or Action | Purpose |
|---|---|
| **Step 16** **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*<br><br>**Example:**<br><br>`Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp` | Creates a dynamic crypto map template and enters the crypto map configuration command mode. |
| **Step 17** **set transform-set** *transform-set-name*<br><br>**Example:**<br><br>`Router(config-crypto-map)# set transform-set aswan` | Specifies which transform sets can be used with the crypto map template. |
| **Step 18** **set isakmp-profile** *profile-name*<br><br>**Example:**<br><br>`Router(config-crypto-map)# set isakmp-profile cisco` | Sets the ISAKMP profile name. |
| **Step 19** **reverse-route [ remote-peer ]**<br><br>**Example:**<br><br>`Router(config-crypto-map)# reverse-route` | Allows routes (ip addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the **remote-peer** keyword for the crypto map. |
| **Step 20** **exit**<br><br>**Example:**<br><br>`Router(config-crypto-map)# exit` | Exits dynamic crypto map configuration mode. |
| **Step 21** crypto map *map-name* ipsec-isakmp dynamic *dynamic-template-name*<br><br>**Example:**<br><br>`Router(config)# crypto map mymap ipsec-isakmp dynamic dmap` | Enters crypto map configuration mode |
| **Step 22** **radius-server hos** t *ip-address* [**auth-port***port-number]* [**acct-port***port-number* ]<br><br>**Example:**<br><br>`Router(config)# radius-server host 172.16.1.4` | Specifies a RADIUS server host. |

| Command or Action | Purpose |
|---|---|
| **Step 23**    **radius-server key** *string* <br><br> **Example:** <br><br> `Router(config)# radius-server key nsite` | Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon. |
| **Step 24**    **radius-server vsa send accounting** <br><br> **Example:** <br><br> `Router(config)# radius-server vsa send accounting` | Configures the network access server to recognize and use vendor-specific attributes. |
| **Step 25**    **interface** *type slot* /*port* <br><br> **Example:** <br><br> `Router(config)# interface FastEthernet 1/0` | Configures an interface type and enters interface configuration mode. |
| **Step 26**    **crypto map** *map-name* <br><br> **Example:** <br><br> `Router(config-if)# crypto map mymap` | Applies a previously defined crypto map set to an interface. |

# Configuring Accounting Updates

To send accounting updates while a session is "up," perform the following optional task:

Before you configure accounting updates, you must first configure IPsec VPN accounting. See the section "Configuring IPsec VPN Accounting, page 14."

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic** *number*

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa accounting update periodic** *number*<br><br>**Example:**<br><br>`Router (config)# aaa accounting update periodic 1-2147483647` | (Optional) Enables periodic interim accounting records to be sent to the accounting server. |

# Troubleshooting for IPsec VPN Accounting

To display messages about IPsec accounting events, perform the following optional task:

### SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp aaa**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **debug crypto isakmp aaa**<br><br>**Example:**<br><br>`Router# debug crypto isakmp aaa` | Displays messages about Internet Key Exchange (IKE) events.<br><br>• The **aaa** keyword specifies accounting events. |

# Configuration Examples for IPsec VPN Accounting

# Accounting and ISAKMP-Profile Example

The following example shows a configuration for supporting remote access clients with accounting and ISAKMP profiles:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2
crypto iakmp client configuration group cclient
 key jegjegjhrg
 pool addressA

crypto-isakmp profile groupA
 vrf cisco
 match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route
!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
```

```
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
 ntp server 172.31.150.52
end
```

# Accounting Without ISAKMP Profiles Example

The following example shows a full Cisco IOS configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
```

```
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
```

```
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

# Additional References

### Related Documents

| Related Topic | Document Title |
| --- | --- |
| Configuring AAA accounting | • Configuring Accounting |
| Configuring IPsec VPN accounting | • Configuring Security for VPNs with IPsec |
| Configuring basic AAA RADIUS | • The section "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide: User Services* on Cisco.com |
| Configuring ISAKMP profiles | VRF Aware IPsec |
| Privilege levels with TACACS+ and RADIUS | • Configuring TACACS+<br>• "Configuring RADIUS" section of the *Cisco IOS Security Configuration Guide: User Services on Cisco.com* |
| IP security, RADIUS, and AAA commands | *Cisco IOS Security Command Reference* |

**MIBs**

| MIBs | MIBs Link |
|---|---|
| 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://www.cisco.com/go/mibs |

**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 |

# Feature Information for IPsec VPN Accounting

The following table provides release information about the feature or features described in this module. This table 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.

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

*Table 4*      *Feature Information for <Phrase Based on Module Title>*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPsec VPN Accounting | 12.2(15)T | The IPsec VPN Accounting feature allows a session to be accounted by indicating when the session starts and stops. A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted. Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server through standard RADIUS attributes and vendor-specific attributes (VSAs).<br><br>This feature was introduced in Cisco IOS Release 12.2(15)T<br><br>The following commands were introduced or modified: **client authentication list, client configuration address, crypto isakmp profile, crypto map (global IPsec), debug crypto isakmp, isakmp authorization list, match identity, set isakmp-profile, vrf** |

# Glossary

**IKE** --Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IP security [IPsec]) that require keys. Before any IPsec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

**IPsec** --IP security. IPsec is A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**ISAKMP** --Internet Security Association and Key Management Protocol. ISAKMP is an Internet IPsec protocol (RFC 2408) that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.

**L2TP session** --Layer 2 Transport Protocol. L2TP are communications transactions between the L2TP access concentrator (LAC) and the L2TP network server (LNS) that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

**NAS** --network access server. A NAS is a Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network [PSTN]).

**PFS** --**perfect forward secrecy. PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.**

**QM** --Queue Manager. The Cisco IP Queue Manager (IP QM) is an intelligent, IP-based, call-treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution.

**RADIUS** --Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

**RSA** --Rivest, Shamir, and Adelman. Rivest, Shamir, and Adelman are the inventors of the Public-key cryptographic system that can be used for encryption and authentication.

**SA** --security association. A SA is an instance of security policy and keying material that is applied to a data flow.

**TACACS**+ --Terminal Access Controller Access Control System Plus. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

**TED** --Tunnel Endpoint Discovery. TED is a Cisco IOS software feature that allows routers to discover IPsec endpoints.

**VPN** --Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

**VRF** --A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**VSA** --vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

**XAUTH** --Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

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.