



IPsec Management Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

Americas Headquarters

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

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2	IP Security VPN Monitoring	3
	Finding Feature Information	3
	Prerequisites for IP Security VPN Monitoring	3
	Restrictions for IP Security VPN Monitoring	4
	Information About IPsec VPN Monitoring	4
	Background Crypto Sessions	4
	Per-IKE Peer Description	4
	Summary Listing of Crypto Session Status	4
	Syslog Notification for Crypto Session Up or Down Status	5
	IKE and IPsec Security Exchange Clear Command	5
	How to Configure IP Security VPN Monitoring	5
	Adding the Description of an IKE Peer	5
	Verifying Peer Descriptions	6
	Clearing a Crypto Session	7
	Configuration Examples for IP Security VPN Monitoring	8
	show crypto session Command Output Examples	8
	Additional References	8
	Related Documents	8
	Standards	9
	MIBs	9
	RFCs	9
	Technical Assistance	9
	Feature Information for IP Security VPN Monitoring	10

CHAPTER 3

IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	11
Finding Feature Information	11
Prerequisites for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	11
Information About IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	12
MIBs Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature	12
SNMP Traps Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature	12
How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	13
How to Troubleshoot the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature	13
Configuration Example for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	14
Configuration That Has Two VRFs Examples	14
Additional References	26
Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	27

CHAPTER 4

IPsec SNMP Support	29
Finding Feature Information	29
Restrictions for IPsec SNMP Support	29
Information About IPsec SNMP Support	30
Related Features and Technologies	30
How to Configure IPsec SNMP Support	31
Enabling IPsec SNMP Notifications	31
Configuring IPsec Failure History Table Size	32
Configuring IPsec Tunnel History Table Size	32
Verifying IPsec MIB Configuration	33
Monitoring and Maintaining IPsec MIB	33
Configuration Examples for IPsec SNMP Support	34
Enabling IPsec Notifications Examples	34
Specifying History Table Size Examples	35
Additional References	35
Feature Information for IPsec SNMP Support	36
Glossary	36

CHAPTER 5

IPsec VPN Accounting	39
-----------------------------	-----------

Finding Feature Information	39
Prerequisites for IPsec VPN Accounting	39
Information About IPsec VPN Accounting	40
RADIUS Accounting	40
RADIUS Start Accounting	40
RADIUS Stop Accounting	41
RADIUS Update Accounting	41
IKE and IPsec Subsystem Interaction	42
Accounting Start	42
Accounting Stop	42
Accounting Updates	43
How to Configure IPsec VPN Accounting	44
Configuring IPsec VPN Accounting	44
Configuring Accounting Updates	48
Troubleshooting for IPsec VPN Accounting	48
Configuration Examples for IPsec VPN Accounting	49
Accounting and ISAKMP-Profile Example	49
Accounting Without ISAKMP Profiles Example	51
Additional References	53
Related Documents	53
Standards	54
MIBs	54
RFCs	54
Technical Assistance	54
Feature Information for IPsec VPN Accounting	54
Glossary	55

CHAPTER 6

IPsec Usability Enhancements	57
Finding Feature Information	57
Prerequisites for IPsec Usability Enhancements	57
Information About IPsec Usability Enhancements	58
IPsec Overview	58
IPsecOperation	58
How to Utilize IPsec Usability Enhancements	59

Verifying IKE Phase-1 ISAKMP Default Policies	59
Default IKE Phase-1 Policies	59
User Configured IKE Policies	60
Easy VPN ISAKMP Policies	60
Verifying Default IPsec Transform-Sets	63
Default Transform Sets	63
Verifying and Troubleshooting IPsec VPNs	64
Verifying IKE Phase-1 ISAKMP	65
Verifying IKE Phase-2	68
Troubleshooting IPsec VPNs	72
Configuration Examples for IPsec Usability Enhancements	74
IKE Default Policies Example	74
Default Transform Sets Example	75
Additional References	76
Feature Information for IPsec Usability Enhancements	78
Glossary	78



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you’re looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).



CHAPTER 2

IP Security VPN Monitoring

The IP Security VPN Monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the Virtual Private Network (VPN) and monitor the end-user interface. Session monitoring enhancements include the following:

- 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, on page 3](#)
 - [Prerequisites for IP Security VPN Monitoring, on page 3](#)
 - [Restrictions for IP Security VPN Monitoring, on page 4](#)
 - [Information About IPsec VPN Monitoring, on page 4](#)
 - [How to Configure IP Security VPN Monitoring, on page 5](#)
 - [Configuration Examples for IP Security VPN Monitoring, on page 8](#)
 - [Additional References, on page 8](#)
 - [Feature Information for IP Security VPN Monitoring, on page 10](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 XE 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. 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

The **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**

Verifying Peer Descriptions

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 {ip-address ip-address} Example: 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 Example: 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 Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show crypto isakmp peer Example: 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
```

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

Command or Action	Purpose
Router# clear crypto session	

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

The following sections provide references related to IP Security VPN Monitoring.

Related Documents

Related Topic	Document Title
IP security, encryption, and IKE	<ul style="list-style-type: none"> Configuring Internet Key Exchange for IPsec VPNs Configuring Security for VPNs with IPsec

Related Topic	Document Title
Security commands	<i>Cisco IOS Security Command Reference</i>

Standards

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

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for exiting MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for exiting RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

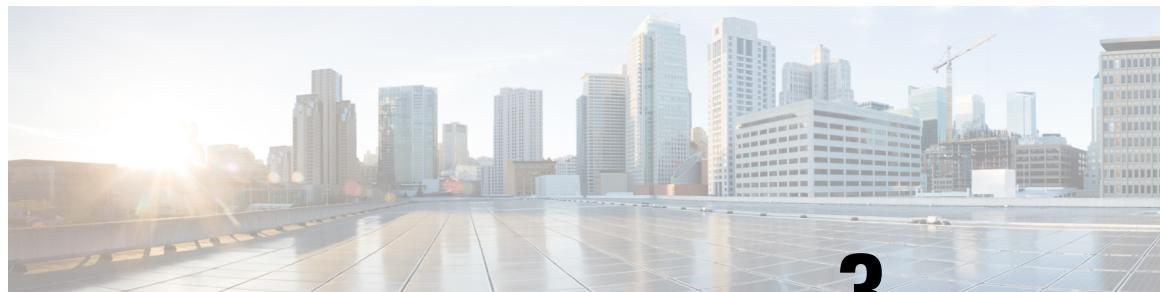
Feature Information for IP Security VPN Monitoring

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	Cisco IOS XE Release 2.1	<p>The IP Security VPN Monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the VPN and monitor the end-user interface. Session monitoring enhancements include the following:</p> <ul style="list-style-type: none"> • Ability to specify an IKE peer description in the configuration file • Summary listing of crypto session status • Syslog notification for crypto session up or down status <p>Ability to clear both IKE and IPsec SAs using one CLI</p> <ul style="list-style-type: none"> • The following commands were introduced or modified: clear crypto session, description (isakmp peer), show crypto isakmp peer, show crypto session.



CHAPTER 3

IPsec and IKE MIB Support forCisco VRF-Aware IPsec

The IPsec and IKE MIB Support for the Virtual Private Network routing and forwarding- (VRF-) aware IP security (IPsec) feature allows VRF-aware IPsec to be managed with MIBs, which provide the details of IPsec statistics and performance metrics on a per VRF basis.

- [Finding Feature Information, on page 11](#)
- [Prerequisites for IPsec and IKE MIB Support forCisco VRF-Aware IPsec, on page 11](#)
- [Information About IPsec and IKE MIB Support forCisco VRF-Aware IPsec, on page 12](#)
- [How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, on page 13](#)
- [Configuration Example for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, on page 14](#)
- [Additional References, on page 26](#)
- [Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, on page 27](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 and IKE MIB Support forCisco VRF-Aware IPsec

- You should be familiar with configuring Simple Network Management Protocol (SNMP).

Information About IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

MIBs Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

- CISCO-IPSEC-FLOW-MONITOR-MIB supports IKE and IPSEC per-tunnel history and failure information. The length of this history and failure information can be configured and must be maintained on a per-VRF basis. The table sizes are controlled by using the **crypto mib ipsec flowmib history tunnel size number** and **crypto mib ipsec flowmib history failure size** commands in global configuration mode.
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB is supported. However, because this MIB applies to the entire router rather than to a specific VPN VRF instance, it is not VRF aware; therefore, polling of the object identifiers (OIDs) that belong to this MIB is accomplished with respect to the global VRF context.

SNMP Traps Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following IKE and IPsec tunnel start and stop traps must go with their corresponding VRF:

- IPSEC_TUNNEL_STOP
- IKE_TUNNEL_STOP
- IPSEC_TUNNEL_START
- IKE_TUNNEL_START

The following traps are global traps that have been modified for the Cisco VRF-Aware IPsec feature:

- TOO_MANY_SAS_CREATED
- CRYPTOMAP_ADDED
- CRYPTOMAPSET_ATTACHED
- CRYPTOMAP_DELETED
- CRYPTOMAPSET_DELETED
- ISAKMP_POLICY_ADDED
- ISAKMP_POLICY_DELETED

How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

No special configuration is needed for this feature. The SNMP framework can be used to manage VRF-aware IPsec using MIBs. See the Configuration Examples for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec section for more information.

The following section provides information about troubleshooting this feature:

How to Troubleshoot the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following **debug crypto mib** command and keywords may be used to display information about the IPsec and Internet Key Exchange (IKE) MIB as it relates to Cisco VRF-aware IPsec.

SUMMARY STEPS

1. **enable**
2. **debug crypto mib detail**
3. **debug crypto mib error**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto mib detail Example: <pre>Router# debug crypto mib detail</pre>	Displays different events as they occur in the IPsec MIB subsystem. <ul style="list-style-type: none"> • Due consideration should be given to enabling debug crypto mib detail because the output for the detail keyword can be quite long.
Step 3	debug crypto mib error Example: <pre>Router# debug crypto mib error</pre>	Displays error events in the MIB agent.

Configuration Example for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

Configuration That Has Two VRFs Examples

The following output example is for a typical hub configuration that has two VRFs. The output is what you would see if you were to poll for the IPsec security association (SA). Router 3745b is the VRF-aware router.

Two VRFs Configured

The following output shows that two VRFs have been configured (vrf1 and vrf2).

```
Router3745b# show running-config
Building configuration...
Current configuration : 6567 bytes
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log uptime
no service password-encryption
!
hostname ipseccf-3745b
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
!
ip vrf vrf1
rd 1:101
context vrf-vrf1-context
route-target export 1:101
route-target import 1:101
!
ip vrf vrf2
rd 2:101
context vrf-vrf2-context
route-target export 2:101
route-target import 2:101
!
no ip domain lookup
!
!
crypto keyring vrf1-1 vrf vrf1
```

```
    pre-shared-key address 10.1.1.1 255.255.255.0 key vrf1-1
crypto keyring vrf2-1 vrf vrf2
    pre-shared-key address 10.1.2.1 255.255.255.0 key vrf2-1
!
!
crypto isakmp policy 1
    authentication pre-share
!
crypto isakmp policy 50
    authentication pre-share
crypto isakmp key global1-1 address 10.1.151.1
crypto isakmp key global2-1 address 10.1.152.1
crypto isakmp profile vrf1-1
    keyring vrf1-1
    match identity address 10.1.1.1 255.255.255.255 vrf1
crypto isakmp profile vrf2-1
    keyring vrf2-1
    match identity address 10.1.2.1 255.255.255.255 vrf2
!
crypto ipsec security-association lifetime kilobytes 99000
crypto ipsec security-association lifetime seconds 5000
!
crypto ipsec transform-set tset ah-sha-hmac esp-des esp-sha-hmac
!
crypto map global1-1 10 ipsec-isakmp
    set peer 10.1.151.1
    set transform-set tset
    match address 151
!
crypto map global2-1 10 ipsec-isakmp
    set peer 10.1.152.1
    set transform-set tset
    match address 152
!
crypto map vrf1-1 10 ipsec-isakmp
    set peer 10.1.1.1
    set transform-set tset
    set isakmp-profile vrf1-1
    match address 101
!
crypto map vrf2-1 10 ipsec-isakmp
    set peer 10.1.2.1
    set transform-set tset
    set isakmp-profile vrf2-1
    match address 102
!
!
interface FastEthernet0/0
    ip address 10.1.38.25 255.255.255.0
    no ip mroute-cache
    duplex auto
    speed auto
!
interface Serial0/0
    no ip address
    shutdown
    clock rate 2000000
!
interface FastEthernet0/1
    no ip address
    no ip mroute-cache
    shutdown
    duplex auto
    speed auto
```

Configuration That Has Two VRFs Examples

```

!
interface Serial0/1
no ip address
shutdown
clock rate 2000000
!
interface Serial1/0
no ip address
encapsulation frame-relay
no ip route-cache cef
no ip route-cache
no ip mroute-cache
no keepalive
serial restart-delay 0
clock rate 128000
no frame-relay inverse-arp
!
interface Serial1/0.1 point-to-point
ip vrf forwarding vrf1
ip address 10.3.1.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 21
!
interface Serial1/0.2 point-to-point
ip vrf forwarding vrf2
ip address 10.3.2.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 22
!
interface Serial1/0.151 point-to-point
ip address 10.7.151.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 151
!
interface Serial1/0.152 point-to-point
ip address 10.7.152.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 152
!
interface Serial1/1
no ip address
no ip mroute-cache
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
encapsulation frame-relay
no ip route-cache cef
no ip route-cache
no ip mroute-cache
no keepalive
serial restart-delay 0
no frame-relay inverse-arp
!
interface Serial1/2.1 point-to-point
ip vrf forwarding vrf1
ip address 10.1.1.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 21
crypto map vrf1-1
!
interface Serial1/2.2 point-to-point
ip vrf forwarding vrf2

```

```

ip address 10.1.2.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 22
crypto map vrf2-1
!
interface Serial1/2.151 point-to-point
ip address 10.5.151.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 151
crypto map global1-1
!
interface Serial1/2.152 point-to-point
ip address 10.5.152.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 152
crypto map global2-1
!
interface Serial1/3
no ip address
no ip mroute-cache
shutdown
serial restart-delay 0
!
ip default-gateway 10.1.38.1
ip classless
ip route 10.1.1.6 255.255.255.255 10.1.151.1
ip route 10.2.1.6 255.255.255.255 10.1.152.1
ip route 10.6.2.1 255.255.255.255 10.7.151.2
ip route 10.6.2.2 255.255.255.255 10.7.152.2
ip route 172.19.216.110 255.255.255.255 FastEthernet0/0
ip route vrf vrf1 10.20.1.1 255.255.255.255 10.1.1.1
ip route vrf vrf1 10.22.1.1 255.255.255.255 10.30.1.1
ip route vrf vrf2 10.20.2.1 255.255.255.255 10.1.2.1
ip route vrf vrf2 10.22.2.1 255.255.255.255 10.30.1.2
!
!
ip http server
no ip http secure-server
!
ip access-list standard vrf-vrf1-context
ip access-list standard vrf-vrf2-context
!
access-list 101 permit ip host 10.22.1.1 host 10.20.1.1
access-list 102 permit ip host 10.22.2.1 host 10.20.2.1
access-list 151 permit ip host 10.6.2.1 host 10.1.1.6
access-list 152 permit ip host 10.6.2.2 host 10.2.1.6
snmp-server group abc1 v2c context vrf-vrf1-context read view_vrf1 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf1-context
snmp-server group abc2 v2c context vrf-vrf2-context read view_vrf2 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf2-context
snmp-server view view_vrf1 iso included
snmp-server view view_vrf2 iso included
snmp-server community abc1 RW
snmp-server community global1 RW
snmp-server community abc2 RW
snmp-server community global2 RW
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.19.216.110 version 2c abc1
snmp-server host 172.19.216.110 vrf vrf1 version 2c abc1 udp-port 2001 ipsec isakmp
snmp-server host 172.19.216.110 version 2c abc2
snmp-server host 172.19.216.110 vrf vrf2 version 2c abc2 udp-port 2002 ipsec isakmp
snmp-server context vrf-vrf1-context
snmp-server context vrf-vrf2-context

```

Configuration That Has Two VRFs Examples

```

!
!
snmp mib community-map abc1 context vrf-vrf1-context
snmp mib community-map abc2 context vrf-vrf2-context
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
webvpn context Default_context
  ssl authenticate verify all
!
no inservice
!
!
end

```

Both VRFs Cleared

The following output, for abc1 and abc2, shows that both VRFs have been “cleared” to ensure that all the counters are initialized to a known value.

The following output shows that VRF abc1 has been cleared:

```

orcasm:2> setenv SR_MGR_CONF /users/green1
orcasm:3> setenv SR_UTIL_SNMP_VERSION v2c
orcasm:5> setenv SR_UTIL_COMMUNITY abc1
orcasm:6> setenv SR_MGR_CONF_DIR /users/green1
orcasm:7> /auto/sw/packages/snmp/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
ciikeGlobalActiveTunnels.0 = 0
ciikeGlobalPreviousTunnels.0 = 0
ciikeGlobalInOctets.0 = 0
ciikeGlobalInPkts.0 = 0
ciikeGlobalInDropPkts.0 = 0
ciikeGlobalInNotifys.0 = 0
ciikeGlobalInP2Exchgs.0 = 0
ciikeGlobalInP2ExchgInvalids.0 = 0
ciikeGlobalInP2ExchgRejects.0 = 0
ciikeGlobalInP2SaDelRequests.0 = 0
ciikeGlobalOutOctets.0 = 0
ciikeGlobalOutPkts.0 = 0
ciikeGlobalOutDropPkts.0 = 0
ciikeGlobalOutNotifys.0 = 0
ciikeGlobalOutP2Exchgs.0 = 0
ciikeGlobalOutP2ExchgInvalids.0 = 0
ciikeGlobalOutP2ExchgRejects.0 = 0
ciikeGlobalOutP2SaDelRequests.0 = 0
ciikeGlobalInitTunnels.0 = 0
ciikeGlobalInitTunnelFails.0 = 0
ciikeGlobalRespTunnelFails.0 = 0
ciikeGlobalSysCapFails.0 = 0
ciikeGlobalAuthFails.0 = 0
ciikeGlobalDecryptFails.0 = 0
ciikeGlobalHashValidFails.0 = 0

```

```

cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIKE TunnelStart.0 = enabled(1)
cipSecTrapCntlIKE TunnelStop.0 = enabled(1)
cipSecTrapCntlIKE SysFailure.0 = disabled(2)
cipSecTrapCntlIKE CertCrlFailure.0 = disabled(2)
cipSecTrapCntlIKE ProtocolFail.0 = disabled(2)
cipSecTrapCntlIKE NoSa.0 = disabled(2)
cipSecTrapCntlIpSec TunnelStart.0 = enabled(1)
cipSecTrapCntlIpSec TunnelStop.0 = enabled(1)
cipSecTrapCntlIpSec SysFailure.0 = disabled(2)
cipSecTrapCntlIpSec SetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSec EarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSec ProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSec NoSa.0 = disabled(2)

```

The following output shows that VRF abc2 has been cleared:

```

orcasm:8> setenv SR_UTIL_COMMUNITY abc2
orcasm:9> /auto/sw/packages/snmpri/14.2.0.0/solaris2bin/getmany -v2c 10.1.38.25 cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotify.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0

```

Configuration That Has Two VRFs Examples

```

cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIKE TunnelStart.0 = enabled(1)
cipSecTrapCntlIKE TunnelStop.0 = enabled(1)
cipSecTrapCntlIKE SysFailure.0 = disabled(2)
cipSecTrapCntlIKE CertCrlFailure.0 = disabled(2)
cipSecTrapCntlIKE ProtocolFail.0 = disabled(2)
cipSecTrapCntlIKE NoSa.0 = disabled(2)
cipSecTrapCntlIpSec TunnelStart.0 = enabled(1)
cipSecTrapCntlIpSec TunnelStop.0 = enabled(1)
cipSecTrapCntlIpSec SysFailure.0 = disabled(2)
cipSecTrapCntlIpSec SetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSec EarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSec ProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSec NoSa.0 = disabled(2)
orcias:10>
orcias:10>
orcias:10>

```

VRF abc1 Pinged

The following output shows that VRF abc1 has been pinged:

```
Router3745a# ping
Protocol [ip]:
Target IP address: 10.22.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.20.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.1.1
```

VRF abc1 Polled

Polling VRF abc1 results in the following output:



Note After the ping, the counters should show some nonzero values.

```
orcasm:10>
orcasm:12> setenv SR_UTIL_COMMUNITY abc1
orcasm:13> /auto/sw/packages/snmpri/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
ciikeGlobalActiveTunnels.0 = 1
ciikeGlobalPreviousTunnels.0 = 0
ciikeGlobalInOctets.0 = 336
ciikeGlobalInPkts.0 = 2
ciikeGlobalInDropPkts.0 = 0
ciikeGlobalInNotifys.0 = 1
ciikeGlobalInP2Exchgs.0 = 2
ciikeGlobalInP2ExchgInvalids.0 = 0
ciikeGlobalInP2ExchgRejects.0 = 0
ciikeGlobalInP2SaDelRequests.0 = 0
ciikeGlobalOutOctets.0 = 344
ciikeGlobalOutPkts.0 = 2
ciikeGlobalOutDropPkts.0 = 0
ciikeGlobalOutNotifys.0 = 0
ciikeGlobalOutP2Exchgs.0 = 1
ciikeGlobalOutP2ExchgInvalids.0 = 0
ciikeGlobalOutP2ExchgRejects.0 = 0
ciikeGlobalOutP2SaDelRequests.0 = 0
ciikeGlobalInitTunnels.0 = 0
ciikeGlobalInitTunnelFails.0 = 0
ciikeGlobalRespTunnelFails.0 = 0
ciikeGlobalSysCapFails.0 = 0
ciikeGlobalAuthFails.0 = 0
ciikeGlobalDecryptFails.0 = 0
ciikeGlobalHashValidFails.0 = 0
ciikeGlobalNoSaFails.0 = 0
```

Configuration That Has Two VRFs Examples

```

cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 4
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 4
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 4
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecTunIkeTunnelIndex.1 = 1
cipSecTunIkeTunnelAlive.1 = true(1)
cipSecTunLocalAddr.1 = 0a 01 01 02
cipSecTunRemoteAddr.1 = 0a 01 01 01
cipSecTunKeyType.1 = ike(1)
cipSecTunEncapMode.1 = tunnel(1)
cipSecTunLifeSize.1 = 99000
cipSecTunLifeTime.1 = 5000
cipSecTunActiveTime.1 = 13749
cipSecTunSaLifeSizeThreshold.1 = 64
cipSecTunSaLifeTimeThreshold.1 = 10
cipSecTunTotalRefreshes.1 = 0
cipSecTunExpiredSaInstances.1 = 0
cipSecTunCurrentSaInstances.1 = 4
cipSecTunInSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunInSaEncryptAlgo.1 = des(2)
cipSecTunInSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunInSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunInSaDecompAlgo.1 = none(1)
cipSecTunOutSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunOutSaEncryptAlgo.1 = des(2)
cipSecTunOutSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaCompAlgo.1 = none(1)
cipSecTunInOctets.1 = 400
cipSecTunHcInOctets.1 = 0x0190
cipSecTunInOctWraps.1 = 0
cipSecTunInDecompOctets.1 = 400
cipSecTunHcInDecompOctets.1 = 0x0190
cipSecTunInDecompOctWraps.1 = 0
cipSecTunInPkts.1 = 4
cipSecTunInDropPkts.1 = 0
cipSecTunInReplayDropPkts.1 = 0
cipSecTunInAuths.1 = 4
cipSecTunInAuthFails.1 = 0
cipSecTunInDecrypts.1 = 4
cipSecTunInDecryptFails.1 = 0
cipSecTunOutOctets.1 = 704
cipSecTunHcOutOctets.1 = 0x02c0
cipSecTunOutOctWraps.1 = 0
cipSecTunOutUncompOctets.1 = 704
cipSecTunHcOutUncompOctets.1 = 0x02c0
cipSecTunOutUncompOctWraps.1 = 0
cipSecTunOutPkts.1 = 4
cipSecTunOutDropPkts.1 = 0
cipSecTunOutAuths.1 = 4
cipSecTunOutAuthFails.1 = 0
cipSecTunOutEncrypts.1 = 4
cipSecTunOutEncryptFails.1 = 0
cipSecTunStatus.1 = active(1)
cipSecEndPtLocalName.1.1 =
cipSecEndPtLocalType.1.1 = singleIpAddr(1)
cipSecEndPtLocalAddr1.1.1 = 16 01 01 01
cipSecEndPtLocalAddr2.1.1 = 16 01 01 01

```

Configuration That Has Two VRFs Examples

```

cipSecEndPtLocalProtocol.1.1 = 0
cipSecEndPtLocalPort.1.1 = 0
cipSecEndPtRemoteName.1.1 =
cipSecEndPtRemoteType.1.1 = singleIpAddr(1)
cipSecEndPtRemoteAddr1.1 = 14 01 01 01
cipSecEndPtRemoteAddr2.1.1 = 14 01 01 01
cipSecEndPtRemoteProtocol.1.1 = 0
cipSecEndPtRemotePort.1.1 = 0
cipSecSpiDirection.1.1 = in(1)
cipSecSpiDirection.1.2 = out(2)
cipSecSpiDirection.1.3 = in(1)
cipSecSpiDirection.1.4 = out(2)
cipSecSpiValue.1.1 = 3891970674
cipSecSpiValue.1.2 = 1963217493
cipSecSpiValue.1.3 = 3691920464
cipSecSpiValue.1.4 = 3458912974
cipSecSpiProtocol.1.1 = ah(1)
cipSecSpiProtocol.1.2 = ah(1)
cipSecSpiProtocol.1.3 = esp(2)
cipSecSpiProtocol.1.4 = esp(2)
cipSecSpiStatus.1.1 = active(1)
cipSecSpiStatus.1.2 = active(1)
cipSecSpiStatus.1.3 = active(1)
cipSecSpiStatus.1.4 = active(1)
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIKE TunnelStart.0 = enabled(1)
cipSecTrapCntlIKE TunnelStop.0 = enabled(1)
cipSecTrapCntlIKE SysFailure.0 = disabled(2)
cipSecTrapCntlIKE CertCrlFailure.0 = disabled(2)
cipSecTrapCntlIKE ProtocolFail.0 = disabled(2)
cipSecTrapCntlIKE NoSa.0 = disabled(2)
cipSecTrapCntlIpSec TunnelStart.0 = enabled(1)
cipSecTrapCntlIpSec TunnelStop.0 = enabled(1)
cipSecTrapCntlIpSec SysFailure.0 = disabled(2)
cipSecTrapCntlIpSec SetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSec EarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSec ProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSec NoSa.0 = disabled(2)
orcias:14>
orcias:14>
orcias:14>
```

VRF abc2 Polled

Polling VRF abc2 results in the following output:



Note

The ping was completed for VRF abc1 only. Therefore, the counters of VRF abc2 should remain in the initialized state.

```

setenv SR_UTIL_COMMUNITY abc2
orcias:15>
orcias:15> /auto/sw/packages/snmp/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
```

```
ciKEGlobalInPkts.0 = 0
ciKEGlobalInDropPkts.0 = 0
ciKEGlobalInNotifys.0 = 0
ciKEGlobalInP2Exchgs.0 = 0
ciKEGlobalInP2ExchgInvalids.0 = 0
ciKEGlobalInP2ExchgRejects.0 = 0
ciKEGlobalInP2SaDelRequests.0 = 0
ciKEGlobalOutOctets.0 = 0
ciKEGlobalOutPkts.0 = 0
ciKEGlobalOutDropPkts.0 = 0
ciKEGlobalOutNotifys.0 = 0
ciKEGlobalOutP2Exchgs.0 = 0
ciKEGlobalOutP2ExchgInvalids.0 = 0
ciKEGlobalOutP2ExchgRejects.0 = 0
ciKEGlobalOutP2SaDelRequests.0 = 0
ciKEGlobalInitTunnels.0 = 0
ciKEGlobalInitTunnelFails.0 = 0
ciKEGlobalRespTunnelFails.0 = 0
ciKEGlobalSysCapFails.0 = 0
ciKEGlobalAuthFails.0 = 0
ciKEGlobalDecryptFails.0 = 0
ciKEGlobalHashValidFails.0 = 0
ciKEGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIKE TunnelStart.0 = enabled(1)
cipSecTrapCntlIKE TunnelStop.0 = enabled(1)
cipSecTrapCntlIKE SysFailure.0 = disabled(2)
cipSecTrapCntlIKE CertCrlFailure.0 = disabled(2)
cipSecTrapCntlIKE ProtocolFail.0 = disabled(2)
cipSecTrapCntlIKE NoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
```

Additional References

```
cipSecTrapCnt1IpSecSysFailure.0 = disabled(2)
cipSecTrapCnt1IpSecSetUpFailure.0 = disabled(2)
cipSecTrapCnt1IpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCnt1IpSecProtocolFail.0 = disabled(2)
cipSecTrapCnt1IpSecNoSa.0 = disabled(2)
orcas:16>
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands by technology	Cisco IOS Release Command References
Cisco IOS master commands list	Master Command List
Configuring SNMP	The chapter “Configuring SNMP Support” in the <i>Cisco IOS Network Management Configuration Guide</i> .
Configuring VRF-Aware IPsec	VRF-Aware IPsec

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • The CISCO-IPSEC-POLICY-MAP-MIB 	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None.	--

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.	http://www.cisco.com/cisco/web/support/index.html
To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.	
Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	

Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

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 2: Feature Information for Feature Information for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

Feature Name	Releases	Feature Information
IPsec and IKE MIB Support for Cisco VRF-Aware IPsec	IOS XE 3.1S	<p>The IPsec and IKE MIB Support for the Virtual Private Network routing and forwarding- (VRF-) aware IP security (IPsec) feature allows VRF-aware IPsec to be managed with MIBs, which provide the details of IPsec statistics and performance metrics on a per VRF basis.</p> <p>This feature was introduced in Cisco IOS Release 12.4(4)T.</p> <p>This feature was integrated into Cisco IOS Release XE 3.1S.</p> <p>The following commands were introduced or modified: debug crypto mib.</p>



CHAPTER 4

IPsec SNMP Support

The IP Security (IPsec) SNMP Support feature introduces support for industry-standard IPsec MIBs and Cisco IOS XE-software specific IPsec MIBs.

The commands in this feature allow you to examine the version of the IPsec MIB feature, to enable and disable SNMP traps, and to monitor and control the size of the buffers used by this feature.



Note This document focuses on Cisco IOS XE CLI support for the Cisco IPsec MIBs. This document also lists which elements of the MIBs are currently supported. This document does not describe SNMP configuration (from a Network Management Station) of the Cisco IPsec MIBs.

- [Finding Feature Information, on page 29](#)
- [Restrictions for IPsec SNMP Support, on page 29](#)
- [Information About IPsec SNMP Support, on page 30](#)
- [How to Configure IPsec SNMP Support, on page 31](#)
- [Configuration Examples for IPsec SNMP Support, on page 34](#)
- [Additional References, on page 35](#)
- [Feature Information for IPsec SNMP Support, on page 36](#)
- [Glossary, on page 36](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

Restrictions for IPsec SNMP Support

- Only the following tunnel setup failure logs are supported with the IPsec--SNMP Support feature:
 - NOTIFY_MIB_IPSEC_PROPOSAL_INVALID

Information About IPsec SNMP Support

- “A tunnel could not be established because the peer did not supply an acceptable proposal.”
- NOTIFY_MIB_IPSEC_ENCRYPT_FAILURE
- “A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.”
- NOTIFY_MIB_IPSEC_SYSCAP_FAILURE
- “A tunnel could not be established because the system ran out of resources.”
- NOTIFY_MIB_IPSEC_LOCAL_FAILURE
- “A tunnel could not be established because of an internal error.”

Note that these failure notices are recorded in the failure tables, but are not available as SNMP notifications (traps).

- The following functions are not supported with the IPsec MIB feature:
 - Checkpointing
 - The Dynamic Cryptomap table of the CISCO-IPSEC-MIB
- The CISCO-IPSEC-POLICY-MAP-MIB (ciscoIpSecPolMap) defines no notifications (the “IPSec Policy Map Notifications Group” is empty).

Information About IPsec SNMP Support

The IP Security (IPsec) SNMP Support feature introduces support for industry-standard IPsec MIBs and Cisco IOS XE-software specific IPsec MIBs.

The IPsec MIBs allow IPsec configuration monitoring and IPsec status monitoring using SNMP, and can be integrated in a variety of Virtual Private Network (VPN) management solutions.

For example, this feature allows you to specify the desired size of a tunnel history table or a tunnel failure table using the Cisco IOS XE CLI. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also provides IPsec Simple Network Management Protocol (SNMP) notifications for use with network management systems.

Related Features and Technologies

The IPsec--SNMP Support feature was designed to support the VPN Device Manager (VDM). VDM enables network administrators to manage and configure site-to-site VPNs on a single device from a web browser and to see the effects of changes in real time. VDM implements a wizard-based graphical user interface (GUI) to simplify the process of configuring site-to-site VPNs using the IPsec protocol. VDM software is installed directly on Cisco VPN routers, and is designed for use and compatibility with future Device Manager products.

How to Configure IPsec SNMP Support

Enabling IPsec SNMP Notifications

To enable IPsec SNMP notifications, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ipsec cryptomap [add | delete | attach | detach]**
4. **snmp-server enable traps isakmp [policy {add | delete} | tunnel {start | stop}]**
5. **snmp-server host host-address traps community-string ipsec**

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	snmp-server enable traps ipsec cryptomap [add delete attach detach] Example: Router (config)# snmp-server enable traps ipsec cryptomap add	Enables a router to send IPsec SNMP notifications.
Step 4	snmp-server enable traps isakmp [policy {add delete} tunnel {start stop}] Example: Router (config)# snmp-server enable traps isakmp policy add	Enables a router to send IPsec ISAKMP SNMP notifications.
Step 5	snmp-server host host-address traps community-string ipsec Example: Router (config)# snmp-server host my.example.com traps version2c	Specifies the recipient of IPsec SNMP notification operations.

What to do next

For more information on configuring SNMP, refer to the chapter “Configuring SNMP Support” in the *Cisco IOS XE Configuration Fundamentals Configuration Guide*.

Configuring IPsec Failure History Table Size

The default failure history table size is 200. To change the size of the failure history table, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history failure size number**

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 mib ipsec flowmib history failure size number Example: Router (config)# crypto mib ipsec flowmib history failure size 220	Changes the size of the IPsec failure history table.

Configuring IPsec Tunnel History Table Size

The default tunnel history table size is 200. To change the size of the tunnel history table, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history tunnel size number**

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 mib ipsec flowmib history tunnel size number Example: Router (config)# crypto mib ipsec flowmib history tunnel size	Changes the size of the IPsec tunnel history table.

Verifying IPsec MIB Configuration

To verify that the IPsec MIB feature is configured properly, perform the following tasks:

- Enter the **show crypto mib ipsec flowmib history failure size** privileged EXEC command to display the size of the failure history table:

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window Size: 140
```

- Enter the **show crypto mib ipsec flowmib history tunnel size** privileged EXEC command to display the size of the tunnel history table:

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

- Enter the **show crypto mib ipsec flowmib version** privileged EXEC command to display the MIB version used by the management applications to identify the feature set:

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

- Enter the **debug crypto mib** command to display the IPsec MIB debug message notifications:

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

Monitoring and Maintaining IPsec MIB

To monitor the status of IPsec MIB information, use any of the following commands.

SUMMARY STEPS

1. enable
2. show crypto mib ipsec flowmib history failure size
3. show crypto mib ipsec flowmib history tunnel size
4. show crypto mib ipsec flowmib version

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show crypto mib ipsec flowmib history failure size Example: Router# show crypto mib ipsec flowmib history failure size	Displays the size of the IPsec failure history table.
Step 3	show crypto mib ipsec flowmib history tunnel size Example: Router# show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPsec tunnel history table.
Step 4	show crypto mib ipsec flowmib version Example: Router# show crypto mib ipsec flowmib version	Displays the IPsec Flow MIB version used by the router.

Configuration Examples for IPsec SNMP Support

Enabling IPsec Notifications Examples

In the following example, IPsec notifications are enabled:

```
snmp-server enable traps ipsec isakmp
```

In the following example, the router is configured to send IPsec notifications to the host nms1.example.com:

```
snmp-server host nms1.example.com public ipsec isakmp
Translating "nms1.example.com"...domain server (172.00.0.01) [OK]
```

Specifying History Table Size Examples

In the following example, the specified failure history table size is 140:

```
crypto mib ipsec flowmib history failure size 140
```

In the following example, the specified tunnel history table size is 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

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 <i>Cisco IOS Security Configuration Guide: User Services</i> on Cisco.com
Configuring ISAKMP profiles	VRF Aware IPsec
Privilege levels with TACACS+ and RADIUS	• Configuring TACACS+ • “Configuring RADIUS” section of the <i>Cisco IOS Security Configuration Guide: User Services on Cisco.com</i>
IP security, RADIUS, and AAA commands	<i>Cisco IOS Security Command Reference</i>
Recommended cryptographic algorithms	Next Generation Encryption

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 SNMP Support

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 3: Feature Information for IPsec SNMP Support

Feature Name	Releases	Feature Information
IPsec SNMP Support	Cisco IOS XE Release 2.1	<p>The IP Security (IPsec) SNMP Support feature introduces support for industry-standard IPsec MIBs and Cisco IOS XE-software specific IPsec MIBs.</p> <p>The following commands were introduced or modified: crypto mib ipsec flowmib history failure size, crypto mib ipsec flowmib history tunnel size, debug crypto mib, show crypto mib ipsec flowmib history failure size, show crypto mib ipsec flowmib history tunnel size, show crypto mib ipsec flowmib version, snmp-server enable traps ipsec, snmp-server enable traps isakmp, snmp-server host.</p>

Glossary

CA --certificate authority. A certificate authority (CA) is an entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Certificates generally include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

IP Security --See IPsec.

IPsec --Internet Protocol Security. 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 Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on

local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to 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.

Management Information Base --See MIB.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Simple Network Management Protocol --See SNMP.

SNMP --Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap --Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.



CHAPTER 5

IPsec VPN Accounting

The IPsec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it 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, on page 39](#)
- [Prerequisites for IPsec VPN Accounting, on page 39](#)
- [Information About IPsec VPN Accounting, on page 40](#)
- [How to Configure IPsec VPN Accounting, on page 44](#)
- [Configuration Examples for IPsec VPN Accounting, on page 49](#)
- [Additional References, on page 53](#)
- [Related Documents, on page 53](#)
- [Feature Information for IPsec VPN Accounting, on page 54](#)
- [Glossary, on page 55](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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

- Understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting.
- Understand 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 4: 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.
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.

RADIUS Attributes	Attribute	Description
Value		
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 5: RADIUS Accounting Stop Packet Attributes

RADIUS Attributes	Attribute	Description
Value		
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.
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=ccclient"
*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-initiator-ip=10.1.2.2"
*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 "username1"
*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-initiator-ip=10.1.1.2"
*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 is configurable. 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-initiator-ip=10.1.1.2"
*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

Before you begin

IPsec must be configured first before configuring IPsec VPN accounting.

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 dynamic-template-name***
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 host *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 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	aaa new-model Example: Router (config)# aaa new-model	Enables periodic interim accounting records to be sent to the accounting server.
Step 4	aaa authentication login <i>list-name method</i> Example: 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 <i>list-name method</i> Example: 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 <i>list-name start-stop [broadcast] group <i>group-name</i></i> Example: Router (config)# aaa accounting network acc start-stop broadcast group radius	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.
Step 7	aaa session-id common Example: 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 <i>profile-name</i> Example: Route (config)# crypto isakmp profile cisco	Audits IP security (IPsec) user sessions and enters isakmp-profile submode.

	Command or Action	Purpose
Step 9	vrf <i>ivrf</i> Example: 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 <i>group-name</i> Example: Router(conf-isa-prof)# match identity group cisco	Matches an identity from a peer in an ISAKMP profile.
Step 11	client authentication list <i>list-name</i> Example: 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 <i>list-name</i> Example: 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 [<i>initiate</i> <i>respond</i>] Example: Router(conf-isa-prof)# client configuration address respond	Configures IKE mode configuration (MODECFG) in the ISAKMP profile.
Step 14	accounting <i>list-name</i> Example: Router(conf-isa-prof)# accounting acc	Enables AAA accounting services for all peers that connect through this ISAKMP profile.
Step 15	exit Example: Router(conf-isa-prof)# exit	Exits isakmp-profile submode.
Step 16	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> Example: 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 <i>transform-set-name</i> Example:	Specifies which transform sets can be used with the crypto map template.

	Command or Action	Purpose
	Router(config-crypto-map) # set transform-set aswan	
Step 18	set isakmp-profile profile-name Example: Router(config-crypto-map) # set isakmp-profile cisco	Sets the ISAKMP profile name.
Step 19	reverse-route [remote-peer] Example: 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 Example: Router(config-crypto-map) # exit	Exits dynamic crypto map configuration mode.
Step 21	crypto map map-name ipsec-isakmp dynamic dynamic-template-name Example: Router(config) # crypto map mymap ipsec-isakmp dynamic dmap	Enters crypto map configuration mode
Step 22	radius-server host ip-address [auth-port port-number] [acct-port port-number] Example: Router(config) # radius-server host 172.16.1.4	Specifies a RADIUS server host.
Step 23	radius-server key string Example: 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 Example: 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 Example: Router(config) # interface FastEthernet 1/0	Configures an interface type and enters interface configuration mode.

Configuring Accounting Updates

	Command or Action	Purpose
Step 26	crypto map <i>map-name</i> Example: <pre>Router(config-if)# crypto map mymap</pre>	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 begin

IPsec VPN accounting must be configured before accounting updates are configured. See [Configuring IPsec VPN Accounting, on page 44](#) for more information.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	aaa accounting update periodic <i>number</i> Example: <pre>Router (config)# aaa accounting update periodic 1-2147483647</pre>	(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 Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto isakmp aaa Example: <pre>Router# debug crypto isakmp aaa</pre>	Displays messages about Internet Key Exchange (IKE) events. <ul style="list-style-type: none"> 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 2.1
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

```

Accounting and ISAKMP-Profile Example

```

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 XE configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```
version 2.1
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
```

Accounting Without ISAKMP Profiles Example

```

        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 ” module in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i>
Configuring IPsec VPN accounting	“ Configuring Security for VPNs with IPsec ” module in the <i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i>
Configuring basic AAA RADIUS	“ Configuring RADIUS ” module in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i>
Configuring ISAKMP profiles	“ VRF-Aware IPsec ” module in the <i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i>
Privilege levels with TACACS+ and RADIUS	<ul style="list-style-type: none"> “ Configuring TACACS+ ” module in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> “ Configuring RADIUS ” module in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i>
IP security, RADIUS, and AAA commands	<i>Cisco IOS Security Command Reference</i>

Standards

Standard	Title
None.	--

MIBs

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

RFCs

RFC	Title
None.	

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	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 6: Feature Information for IPsec VPN Accounting

Feature Name	Releases	Feature Information
IPsec VPN Accounting	Cisco IOS XE Release 2.1	<p>The IPsec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops.</p> <p>A VPN session is defined as an IKE SA and the one or more SA pairs that are created by the IKE SA. The session starts when the first IPsec pair is created and stops when all IPsec SAs are deleted.</p> <p>Session identifying information and session usage information is passed to the RADIUS server through standard RADIUS attributes and VSAs.</p> <p>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.</p>

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.

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).



CHAPTER 6

IPsec Usability Enhancements

The IPsec Usability Enhancements feature introduces functionality that eases the configuration and monitoring of your IPsec virtual private network (VPN). Benefits of this feature include intelligent defaults for IPsec and Internet Key Exchange (IKE) and the ability to easily verify and troubleshoot IPsec VPNs.

- [Finding Feature Information, on page 57](#)
- [Prerequisites for IPsec Usability Enhancements, on page 57](#)
- [Information About IPsec Usability Enhancements, on page 58](#)
- [How to Utilize IPsec Usability Enhancements, on page 59](#)
- [Configuration Examples for IPsec Usability Enhancements, on page 74](#)
- [Additional References, on page 76](#)
- [Feature Information for IPsec Usability Enhancements, on page 78](#)
- [Glossary, on page 78](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 Usability Enhancements

- You must be familiar with IPsec, IKE, and encryption.
- You must have configured IPsec and enabled IKE on your router.
- You must be running Cisco IOS XE k9 crypto image on your router.

Information About IPsec Usability Enhancements

IPsec Overview

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF), which provides security for transmission of sensitive information over public networks. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

IPsec provides secure tunnels between two peers. You may define which packets are considered sensitive and should be sent through these secure tunnels. You may also define the parameters that should be used to protect these sensitive packets by specifying characteristics of the tunnels. When an IPsec peer detects a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

IPsec Operation

An IPsec operation involves five basic steps: identifying interesting traffic, IKE phase-1, IKE phase-2, establishing the tunnel or IPsec session, and finally tearing down the tunnel.

Step 1: Identifying Interesting Traffic

The VPN devices recognize the traffic, or sensitive packets, to detect. IPsec is either applied to the sensitive packet, the packet is bypassed, or the packet is dropped. Based on the traffic type, if IPsec is applied then IKE phase-1 is initiated.

Step 2: IKE Phase-1

There are three exchanges between the VPN devices to negotiate an IKE security policy and establish a secure channel.

During the first exchange, the VPN devices negotiate matching IKE transform sets to protect the IKE exchange resulting in establishing an Internet Security Association and Key Management Protocol (ISAKMP) policy to utilize. The ISAKMP policy consists of an encryption algorithm, a hash algorithm, an authentication algorithm, a Diffie-Hellman (DH) group, and a lifetime parameter.

There are eight default ISAKMP policies supported. For more information on default ISAKMP policies, see the [Verifying IKE Phase-1 ISAKMP Default Policies, on page 59](#).

The second exchange consists of a Diffie-Hellman exchange, which establishes a shared secret.

The third exchange authenticates peer identity. After the peers are authenticated, IKE phase-2 begins.

Step 3: IKE Phase-2

The VPN devices negotiate the IPsec security policy used to protect the IPsec data. IPsec transform sets are negotiated.

A transform set is a combination of algorithms and protocols that enact a security policy for network traffic. For more information on default transform sets, see the [Verifying Default IPsec Transform-Sets, on page 63](#). A VPN tunnel is ready to be established.

Step 4: Establishing the Tunnel--IPsec Session

The VPN devices apply security services to IPsec traffic and then transmit the IPsec data. Security associations (SAs) are exchanged between peers. The negotiated security services are applied to the tunnel traffic while the IPsec session is active.

Step 5: Terminating the Tunnel

The tunnel is torn down when an IPsec SA lifetime time-out occurs or if the packet counter is exceeded. The IPsec SA is removed.

How to Utilize IPsec Usability Enhancements

Verifying IKE Phase-1 ISAKMP Default Policies

When IKE negotiation begins, the peers try to find a common policy, starting with the highest priority policy as specified on the remote peer. The peers negotiate the policy sets until there is a match. If peers have more than one policy set in common, the lowest priority number is used.

There are three groups of IKE phase-1, ISAKMP, policies as defined by policy priority ranges and behavior:

- Default ISAKMP policies, which are automatically enabled.
- User configured ISAKMP policies, which you may configure with the **crypto isakmp policy** command.
- Easy VPN ISAKMP policies, which are made available during Easy VPN configuration.

This section describes the three groups of ISAKMP policies, how they behave in relationship to one another, how to determine which policies are in use with the appropriate **show** command, and how to disable the default ISAKMP policies.

Default IKE Phase-1 Policies

There are eight default IKE phase-1, ISAKMP, policies supported (see the table below) that are enabled automatically. If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor disabled the default IKE policies with the **no crypto isakmp default policy** command, the default IKE policies will be used during peer IKE negotiations. You can verify that the default IKE policies are in use by issuing either the **show crypto isakmp policy** command or the **show crypto isakmp default policy** command.



Note

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

The default IKE policies define the following policy set parameters:

- The priority, 65507-65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).

User Configured IKE Policies

- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The DH group specification DH2 or DH5
 - DH2 specifies the 768-bit DH group.
 - DH5 specifies the 1536-bit DH group.



Note Cisco no longer recommends using 3DES, MD5 and DH groups 1, 2 and 5. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption \(NGE\)](#) white paper. To learn more about IKE configuration, read the chapter “Configuring Internet Key Exchange for IPsec VPNs” in *Internet Key Exchange for IPsec VPNs Configuration Guide*.

Table 7: Default IKE Phase-1, ISAKMP, Policies

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

User Configured IKE Policies

You may configure IKE policies with the **crypto isakmp policy** command. User configured IKE policies are uniquely identified and configured with a priority number ranging from 1-10000, where 1 is the highest priority and 10000 the lowest priority.

Once you have configured one or more IKE policies with a priority of 1-10000:

- The user configured policies will be used during peer IKE negotiations.
- The default IKE policies will no longer used during peer IKE negotiations.
- The user configured policies may be displayed by issuing the **show crypto isakmp policy** command.

Easy VPN ISAKMP Policies

If you have configured Easy VPN, the default Easy VPN ISAKMP policies in use are uniquely identified with a priority number ranging from 65515-65535, where 65515 is the highest priority and 65535 is the lowest priority.

Once a user has configured Easy VPN:

- The default Easy VPN ISAKMP policies and the default IKE policies will be used during peer IKE negotiations.
- The Easy VPN ISAKMP policies and the default IKE policies will be displayed by issuing the **show crypto isakmp policy** command.
- Default ISAKMP policies will be displayed by issuing the **show crypto isakmp default policy** command unless they have been disabled by issuing the **no crypto isakmp default policy** command.

SUMMARY STEPS

- enable**
- show crypto isakmp default policy**
- configure terminal**
- no crypto isakmp default policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show crypto isakmp default policy Example: Router# show crypto isakmp default policy	(Optional) Displays default ISAKMP policies if no policy with a priority of 1-10000 is configured.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	no crypto isakmp default policy Example: Router(config)# no crypto isakmp default policy	(Optional) Turns off default ISAKMP policies with priorities 65507-65514.

Examples

The following is sample output of the **show crypto isakmp default policy** command. The default policies are displayed because the default policies have not been disabled.

```
Router# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
    encryption algorithm: AES - Advanced Encryption Standard (128 bit key).
```

```

        hash algorithm: Secure Hash Standard
        authentication method: Rivest-Shamir-Adleman Signature
        Diffie-Hellman group: #5 (1536 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm: AES - Advanced Encryption Standard (128 bit key.
        hash algorithm: Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group: #5 (1536 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm: AES - Advanced Encryption Standard (128 bit key.
        hash algorithm: Message Digest 5
        authentication method: Rivest-Shamir-Adleman Signature
        Diffie-Hellman group: #5 (1536 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm: AES - Advanced Encryption Standard (128 bit key.
        hash algorithm: Message Digest 5
        authentication method: Pre-Shared Key
        Diffie-Hellman group: #5 (1536 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm: Three key triple DES
        hash algorithm: Secure Hash Standard
        authentication method: Rivest-Shamir-Adleman Signature
        Diffie-Hellman group: #2 (1024 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm: Three key triple DES
        hash algorithm: Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group: #2 (1024 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm: Three key triple DES
        hash algorithm: Message Digest 5
        authentication method: Rivest-Shamir-Adleman Signature
        Diffie-Hellman group: #2 (1024 bit)
        lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm: Three key triple DES
        hash algorithm: Message Digest 5
        authentication method: Pre-Shared Key
        Diffie-Hellman group: #2 (1024 bit)
        lifetime: 86400 seconds, no volume limit

```

The following example disables the default IKE policies then shows the resulting output of the **show crypto isakmp default policy** command, which is blank:

```

Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.

```

The following is an example system log message that is generated whenever the default ISAKMP policies are in use:

```
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

Verifying Default IPsec Transform-Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

During IPsec SA negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and is applied to the protected traffic as part of the IPsec SAs of both peers.

Default Transform Sets

A default transform set will be used by any crypto map or IPsec profile where no other transform set has been configured and if the following is true:

- The default transform sets have not been disabled with the **no crypto ipsec default transform-set** command.
- The crypto engine in use supports the encryption algorithm.

The two default transform sets each define an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type as shown in the table below.

Table 8: Default Transform Sets and Parameters

Default Transform Name	ESP Encryption Transform and Description	ESP Authentication Transform and Description
#\$!default_transform_set_0	esp-3des (ESP with the 168-bit 3DES or Triple DES encryption algorithm)	esp-sha-hmac
#\$!default_transform_set_1	esp-aes (ESP with the 128-bit AES encryption algorithm)	esp-sha-hmac (ESP with the SHA-1, hash message authentication code [HMAC] variant authentication algorithm)

SUMMARY STEPS

1. **enable**
2. **show crypto ipsec default transform-set**
3. **configure terminal**
4. **no crypto ipsec default transform-set**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	show crypto ipsec default transform-set Example: Router# show crypto ipsec default transform-set	(Optional) Displays the default IPsec transform sets currently in use by IKE.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	no crypto ipsec default transform-set Example: Router(config)# no crypto ipsec default transform-set	(Optional) Disables the default IPsec transform sets.

Examples

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets are enabled, the default setting:

```
Router# show crypto ipsec default transform-set
Transform set #$/default_transform_set_1: { esp-aes esp-sha-hmac }
    will negotiate = { Transport, },
Transform set #$/default_transform_set_0: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, },
```

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default transform-set** command.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

The following is an example system log message that is generated whenever IPsec SAs have negotiated with a default transform set:

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPsec transform-set
```

Verifying and Troubleshooting IPsec VPNs

Perform one of the following optional tasks in this section, depending on whether you want to verify IKE phase-1 or IKE phase-2 tunnels or troubleshoot your IPsec VPN:

Verifying IKE Phase-1 ISAKMP

To display statistics for ISAKMP tunnels, use the following optional commands.

SUMMARY STEPS

1. **show crypto mib isakmp flowmib failure [vrf *vrf-name*]**
2. **show crypto mib isakmp flowmib global [vrf *vrf-name*]**
3. **show crypto mib isakmp flowmib history [vrf *vrf-name*]**
4. **show crypto mib isakmp flowmib peer [index *peer-mib-index*] [vrf *vrf-name*]**
5. **show crypto mib isakmp flowmib tunnel [index *tunnel-mib-index*] [vrf *vrf-name*]**

DETAILED STEPS

Step 1 **show crypto mib isakmp flowmib failure [vrf *vrf-name*]**

For ISAKMP tunnel failures, this command displays event information. The following is sample output for this command:

Example:

```
Router# show crypto mib isakmp flowmib failure
vrf Global
Index: 1
Reason: peer lost
Failure time since reset: 00:07:27
Local type: ID_IPV4_ADDR
Local value: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote Value: 192.0.2.2
Local Address: 192.0.2.1
Remote Address: 192.0.2.2
Index: 2
Reason: peer lost
Failure time since reset: 00:07:27
Local type: ID_IPV4_ADDR
Local value: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote Value: 192.0.3.2
Local Address: 192.0.3.1
Remote Address: 192.0.3.2
Index: 3
Reason: peer lost
Failure time since reset: 00:07:32
Local type: ID_IPV4_ADDR
Remote type: ID_IPV4_ADDR
Remote Value: 192.0.2.2
Local Address: 192.0.2.1
Remote Address: 192.0.2.2
```

Step 2 **show crypto mib isakmp flowmib global [vrf *vrf-name*]**

Global ISAKMP tunnel statistics are displayed by issuing this command. The following is sample output for this command:

Example:

```
Router# show crypto mib isakmp flowmib global
vrf Global
Active Tunnels: 3
```

Verifying IKE Phase-1 ISAKMP

Previous Tunnels:	0
In octets:	2856
Out octets:	3396
In packets:	16
Out packets:	19
In packets drop:	0
Out packets drop:	0
In notifys:	4
Out notifys:	7
In P2 exchg:	3
Out P2 exchg:	6
In P2 exchg invalids:	0
Out P2 exchg invalids:	0
In P2 exchg rejects:	0
Out P2 exchg rejects:	0
In IPSEC delete:	0
Out IPSEC delete:	0
SAs locally initiated:	3
SAs locally initiated failed:	0
SAs remotely initiated failed:	0
System capacity failures:	0
Authentication failures:	0
Decrypt failures:	0
Hash failures:	0
Invalid SPI:	0

Step 3 show crypto mib isakmp flowmib history [vrf *vrf-name*]

For information about ISAKMP tunnels that are no longer active, this command displays event information including the reason that the tunnel was terminated. The following is sample output for this command:

Example:

```
Router# show crypto mib isakmp flowmib history
vrf Global
Reason: peer lost
Index: 2
Local type: ID_IPV4_ADDR
Local address: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.2.2
Negotiation mode: Main Mode
Diffie Hellman Grp: 2
Encryption algo: des
Hash algo: sha
Auth method: psk
Lifetime: 86400
Active time: 00:06:30
Policy priority: 1
Keepalive enabled: Yes
In octets: 3024
In packets: 22
In drops: 0
In notifys: 18
In P2 exchanges: 1
In P2 exchg invalids: 0
In P2 exchg rejected: 0
In P2 SA delete reqs: 0
Out octets: 4188
Out packets: 33
Out drops: 0
Out notifys: 28
Out P2 exchgs: 2
Out P2 exchg invalids: 0
```

```

Out P2 exchg rejects: 0
Out P2 Sa delete requests: 0
Reason: peer lost
Index: 3
Local type: ID_IPV4_ADDR
Local address: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.3.2
Negotiation mode: Main Mode
Diffie Hellman Grp: 2
Encryption algo: des
Hash algo: sha
Auth method: psk
Lifetime: 86400
Active time: 00:06:25
Policy priority: 1
Keepalive enabled: Yes
In octets: 3140
In packets: 23
In drops: 0
In notifys: 19
In P2 exchanges: 1
In P2 exchg invalids: 0
In P2 exchg rejected: 0
In P2 SA delete reqs: 0
Out octets: 4304
Out packets: 34
Out drops: 0
Out notifys: 29
Out P2 exchgs: 2
Out P2 exchg invalids: 0
Out P2 exchg rejects: 0
Out P2 Sa delete requests: 0

```

Step 4 show crypto mib isakmp flowmib peer [index *peer-mib-index*] [vrf *vrf-name*]

For active ISAKMP peer associations, this command displays information including indexes, type of connection, and IP addresses. The following is sample output for this command:

Example:

```

Router# show crypto mib isakmp flowmib peer
vrf Global
Index: 1
Local type: ID_IPV4_ADDR
Local address: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.2.2
Index: 2
Local type: ID_IPV4_ADDR
Local address: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.3.1
Index: 3
Local type: ID_IPV4_ADDR
Local address: 192.0.4.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.4.1

```

Step 5 show crypto mib isakmp flowmib tunnel [index *tunnel-mib-index*] [vrf *vrf-name*]

For active ISAKMP tunnels, this command displays tunnel statistics. The following is sample output for this command:

Example:

Verifying IKE Phase-2

```
Router# show crypto mib isakmp flowmib tunnel
vrf Global
  Index: 1
  Local type: ID_IPV4_ADDR
  Local address: 192.0.2.1
  Remote type: ID_IPV4_ADDR
  Remote address: 192.0.2.2
  Negotiation mode: Main Mode
  Diffie Hellman Grp: 2
  Encryption algo: des
  Hash algo: sha
  Auth method: psk
  Lifetime: 86400
  Active time: 00:03:08
  Policy priority: 1
  Keepalive enabled: Yes
  In octets: 2148
  In packets: 15
  In drops: 0
  In notifys: 11
  In P2 exchanges: 1
  In P2 exchg invalids: 0
  In P2 exchg rejected: 0
  In P2 SA delete reqs: 0
  Out octets: 2328
  Out packets: 16
  Out drops: 0
  Out notifys: 12
  Out P2 exchgs: 2
  Out P2 exchg invalids: 0
  Out P2 exchg rejects: 0
  Out P2 Sa delete requests: 0
```

Verifying IKE Phase-2

To display statistics for IPsec phase-2 tunnels, use the following optional commands.

SUMMARY STEPS

1. **show crypto mib ipsec flowmib endpoint [vrf *vrf-name*]**
2. **show crypto mib ipsec flowmib failure [vrf *vrf-name*]**
3. **show crypto mib ipsec flowmib global [vrf *vrf-name*]**
4. **show crypto mib ipsec flowmib history [vrf *vrf-name*]**
5. **show crypto mib ipsec flowmib spi [vrf *vrf-name*]**
6. **show crypto mib ipsec flowmib tunnel [index *tunnel-mib-index*] [vrf *vrf-name*]**

DETAILED STEPS**Step 1 show crypto mib ipsec flowmib endpoint [vrf *vrf-name*]**

Information for each active endpoint, local or remote device, associated with an IPsec phase-2 tunnel is displayed by issuing this command. The following is sample output for this command:

Example:

```
Router# show crypto mib ipsec flowmib endpoint
vrf Global
  Index: 1
  Local type: Single IP address
  Local address: 192.1.2.1
  Protocol: 0
  Local port: 0
  Remote type: Single IP address
  Remote address: 192.1.2.2
  Remote port: 0
  Index: 2
  Local type: Subnet
  Local address: 192.1.3.0 255.255.255.0
  Protocol: 0
  Local port: 0
  Remote type: Subnet
  Remote address: 192.1.3.0 255.255.255.0
  Remote port: 0
```

Step 2 show crypto mib ipsec flowmib failure [vrf vrf-name]

For ISAKMP tunnel failures, this command displays event information. The following is sample output for this command:

Example:

```
Router# show crypto mib ipsec flowmib failure
vrf Global
  Index: 1
  Reason: Operation request
  Failure time since reset: 00:25:18
  Src address: 192.1.2.1
  Destination address: 192.1.2.2
  SPI: 0
```

Step 3 show crypto mib ipsec flowmib global [vrf vrf-name]

Global IKE phase-2 tunnel statistics are displayed by issuing this command. The following is sample output for this command:

Example:

```
Router# show crypto mib ipsec flowmib global
vrf Global
  Active Tunnels: 2
  Previous Tunnels: 0
  In octets: 800
  Out octets: 1408
  In packets: 8
  Out packets: 8
  Uncompressed encrypted bytes: 1408
  In packets drops: 0
  Out packets drops: 2
  In replay drops: 0
  In authentications: 8
  Out authentications: 8
  In decrypts: 8
  Out encrypts: 8
  Compressed bytes: 0
  Uncompressed bytes: 0
  In uncompressed bytes: 0
  Out uncompressed bytes: 0
  In decrypt failures: 0
```

Verifying IKE Phase-2

```

Out encrypt failures:          0
No SA failures:              0
! Number of SA Failures.
Protocol use failures:       0
System capacity failures:    0
In authentication failures:   0
Out authentication failures:  0

```

Step 4 show crypto mib ipsec flowmib history [vrf *vrf-name*]

For information about IKE phase-2 tunnels that are no longer active, this command displays event information including the reason that the tunnel was terminated. The following is sample output for this command:

Example:

```

Router# show crypto mib ipsec flowmib history
vrf Global
Reason:                      Operation request
Index:                       1
Local address:                192.1.2.1
Remote address:               192.1.2.2
IPSEC keying:                 IKE
Encapsulation mode:          1
Lifetime (KB):                4608000
Lifetime (Sec):                3600
Active time:                  00:24:32
Lifetime threshold (KB):      423559168
Lifetime threshold (Sec):     3590000
Total number of refreshes:   0
Expired SA instances:        4
Current SA instances:        4
In SA DH group:              14
In sa encrypt algorithm:     aes
In SA auth algorithm:        rsig
In SA ESP auth algo:         ESP_HMAC_SHA
In SA uncompress algorithm:  None
Out SA DH group:              14
Out SA encryption algorithm: aes
Out SA auth algorithm:       ESP_HMAC_SHA
Out SA ESP auth algorithm:   ESP_HMAC_SHA
Out SA uncompress algorithm: None
In octets:                   400
Decompressed octets:         400
In packets:                  4
In drops:                     0
In replay drops:              0
In authentications:           4
In authentication failures:   0
In decrypts:                  4
In decrypt failures:          0
Out octets:                   704
Out uncompressed octets:     704
Out packets:                  4
Out drops:                     1
Out authentications:           4
Out authentication failures:   0
Out encrypts:                  4
Out encryption failures:      0
Compressed octets:             0
Decompressed octets:           0
Out uncompressed octets:      704

```

Step 5 show crypto mib ipsec flowmib spi [vrf *vrf-name*]

The security protection index (SPI) table contains an entry for each active and expiring security IKE phase-2 association. The following is sample output for this command, which displays the SPI table:

Example:

```
Router# show crypto mib ipsec flowmib spi
vrf Global
  Tunnel Index:          1
  SPI Index:            1
  SPI Value:             0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            2
  SPI Value:             0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            3
  SPI Value:             0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active
  SPI Index:            4
  SPI Value:             0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

Step 6 show crypto mib ipsec flowmib tunnel [index tunnel-mib-index] [vrf vrf-name]

For active IKE phase-2 tunnels, this command displays tunnel statistics. The following is sample output for this command:

Example:

```
Router# show crypto mib ipsec flowmib tunnel
vrf Global
  Index:                      1
  Local address:              192.0.2.1
  Remote address:             192.0.2.2
  IPSEC keying:               IKE
  Encapsulation mode:         1
  Lifetime (KB):              4608000
  Lifetime (Sec):             3600
  Active time:                00:05:46
  Lifetime threshold (KB):    64
  Lifetime threshold (Sec):   10
  Total number of refreshes:  0
  Expired SA instances:       0
  Current SA instances:      4
  In SA DH group:            14
  In sa encrypt algorithm:   aes
  In SA auth algorithm:     rsig
  In SA ESP auth algo:      ESP_HMAC_SHA
  In SA uncompress algorithm: None
  Out SA DH group:           14
  Out SA encryption algorithm: aes
  Out SA auth algorithm:    ESP_HMAC_SHA
  Out SA ESP auth algorithm: ESP_HMAC_SHA
  Out SA uncompress algorithm: None
  In octets:                  400
  Decompressed octets:       400
  In packets:                 4
```

In drops:	0
In replay drops:	0
In authentications:	4
In authentication failures:	0
In decrypts:	4
In decrypt failures:	0
Out octets:	704
Out uncompressed octets:	704
Out packets:	4
Out drops:	1
Out authentications:	4
Out authentication failures:	0
Out encryptions:	4
Out encryption failures:	0
Compressed octets:	0
Decompressed octets:	0
Out uncompressed octets:	704

Troubleshooting IPsec VPNs

The **show tech-support ipsec** command simplifies the collection of the IPsec related information if you are troubleshooting a problem.

SUMMARY STEPS

1. **show tech-support ipsec**

DETAILED STEPS

show tech-support ipsec

There are three variations of the **show tech-support ipsec** command:

- **show tech-support ipsec**
- **show tech-support ipsec peer *ipv4address***
- **show tech-support ipsec vrf *vrf-name***

For a sample display of the output from the **show tech-support ipsec** command for the individual **show** commands listed below for each variation see the following sections.

Output of the show tech-support ipsec Command

If you enter the **show tech-support ipsec** command without any keywords, the command output displays the following **show** commands, in order of output:

- **show version**
- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**

- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

Output of the show tech-support ipsec peer Command

If you enter the **show tech-support ipsec** command with the **peer** keyword and the *ipv4address* argument, the output displays the following **show** commands, in order of output for the specified peer:

- **show version**
- **show running-config**
- **show crypto session remote *ipv4address* detail**
- **show crypto isakmp sa peer *ipv4address* detail**
- **show crypto ipsec sa peer *ipv4address* detail**
- **show crypto isakmp peers *ipv4address***
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

Output of the show tech-support ipsec vrf Command

If you enter the **show tech-support ipsec** command with the **vrf** keyword and the *vrf-name* argument, the output displays the following **show** commands, in order of output for the specified Virtual Routing and Forwarding (VRF):

- **show version**
- **show running-config**
- **show crypto isakmp sa count vrf *vrf-name***
- **show crypto ipsec sa count vrf *vrf-name***
- **show crypto session ivrf *ivrf-name* detail**
- **show crypto session fvrf *fvrif-name* detail**

- show crypto isakmp sa vrf *vrf-name* detail
- show crypto ipsec sa vrf *vrf-name* detail
- show crypto ruleset detail
- show processes memory | include Crypto IKMP
- show processes cpu | include Crypto IKMP
- show crypto eli
- show crypto engine accelerator statistic

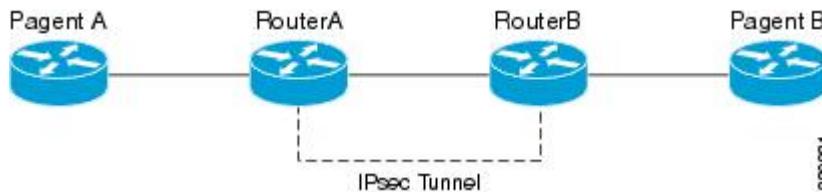
Example:

Configuration Examples for IPsec Usability Enhancements

IKE Default Policies Example

In the following example, crypto maps are configured on RouterA and RouterB and default IKE policies are in use. Traffic is routed from Pagent A to Pagent B. Checking the system log on Peer A and Peer B confirms that the default IKE policies are in use on both peers (see the figure below).

Figure 1: Example Site to Site Topology



```

! Configuring RouterA.
RouterA(config)# crypto isakmp key identity address 209.165.200.226
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.226
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.226
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.225
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterA(cfg-crypto-trans)# mode tunnel
RouterA(cfg-crypto-trans)# end
RouterA(config)# crypto map testmap 10
RouterA(config-crypto-map)# set transform-set test_transf
  
```

```

RouterA(config-crypto-map)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.228
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.228
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterB(cfg-crypto-trans)# mode tunnel
RouterB(cfg-crypto-trans)# end
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# set transform-set test_transf
RouterB(config-crypto-map)# end
! Routing traffic from PagentA to PagentB.
PagentA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.229
PagentA(config)# end
! Routing traffic from PagentB to PagentA.
PagentB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.230
PagentB(config)# end
! Checking the system log on RouterA confirms that the default IKE policies are in use.
RouterA# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun 5 09:17:59.251 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
! Checking the system log on RouterB confirms that the default IKE policies are in use.
RouterB# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun 5 09:17:59.979 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies

```

Default Transform Sets Example

In the following example, static crypto maps are configured on RouterA and dynamic crypto maps are configured on RouterB. Traffic is routed from Pagent A to Pagent B. The IPsec SAs negotiate with default transform sets and the traffic is encrypted. Executing the **show crypto map** command on both peers verifies that the default transform sets are in use.

```

! Configuring RouterA.
RouterA(config)# crypto isakmp key identify address 209.165.200.225
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.225
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.226 255.255.255.255 209.165.200.225
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto isakmp policy 10
RouterA(config-isakmp)# encryption aes
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# hash sha
RouterA(config-isakmp)# group 5
RouterA(config-isakmp)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.229
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap

```

Additional References

```

RouterB(config)# ip route 209.165.200.227 255.255.255.255 209.165.200.229
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto isakmp policy 10
RouterB(config-isakmp)# encryption aes
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# hash sha
RouterB(config-isakmp)# group 5
RouterB(config-isakmp)# end
! The SA is using the default transform set and traffic is encrypted on RouterA.
RouterA# show crypto isakmp sa detail | include 209.165.200.229.*209.165.200.225.*ACTIVE
13007 209.165.200.229      209.165.200.225      ACTIVE aes sha psk 5 23:59:56
13006 209.165.200.229      209.165.200.225      ACTIVE aes sha psk 5 0
13005 209.165.200.229      209.165.200.225      ACTIVE aes sha psk 5 0
! The SA is using the default transform set and traffic is encrypted on RouterB.
RouterB# show crypto isakmp sa detail | include 209.165.200.225.*209.165.200.229.*ACTIVE
7007 209.165.200.225      209.165.200.229      ACTIVE aes sha psk 5 23:59:55
7006 209.165.200.225      209.165.200.229      ACTIVE aes sha psk 5 0
7005 209.165.200.225      209.165.200.229      ACTIVE aes sha psk 5 0
! Verifying that the default transform sets are in use on RouterA.
RouterA# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
Peer = 209.165.200.225
Extended IP access list 101
    access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
Current peer: 209.165.200.225
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
    #$_!default_transform_set_1: { esp-aes esp-sha-hmac } ,
    #$_!default_transform_set_0: { esp-3des esp-sha-hmac } ,
}
Interfaces using crypto map testmap:
FastEthernet1/2
! Verifying that the default transform sets are in use on RouterB.
RouterB# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
Dynamic map template tag: dyn_testmap
Crypto Map "testmap" 65536 ipsec-isakmp
Peer = 209.165.200.229
Extended IP access list
    access-list permit ip host 209.165.200.226 host 209.165.200.227
        dynamic (created from dynamic map dyn_testmap/10)
Current peer: 209.165.200.229
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={
    #$_!default_transform_set_1: { esp-aes esp-sha-hmac } ,
}
Interfaces using crypto map testmap:
GigabitEthernet0/1

```

Additional References

The following sections provide references related to the IPsec Usability Enhancement feature.

Related Documents

Related Topic	Document Title
IKE configuration	Configuring Internet Key Exchange for IPsec VPNs module in the <i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i>
IPsec configuration	Configuring Security for VPNs with IPsec module in the <i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i>
Easy VPN server	Easy VPN Server module in the <i>Cisco IOS XE Security Configuration Guide: Secure Connectivity</i>
Cisco IOS XE security commands	<i>Cisco IOS Security Command Reference</i>

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for IPsec Usability Enhancements

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 9: Feature Information for IPsec Usability Enhancements

Feature Name	Releases	Feature Information
IPsec Usability Enhancements	Cisco IOS XE Release 2.4	<p>This feature introduces intelligent defaults for IKE and IPsec, and show commands to access MIB statistics and to aid in troubleshooting.</p> <p>The following commands were introduced or modified: crypto ipsec default transform-set, crypto isakmp default policy, crypto isakmp policy, show crypto ipsec default transform-set, show crypto ipsec transform-set, show crypto isakmp default policy, show crypto isakmp policy, show crypto map (IPsec), show crypto mib ipsec flowmib endpoint, show crypto mib ipsec flowmib failure, show crypto mib ipsec flowmib global, show crypto mib ipsec flowmib history, show crypto mib ipsec flowmib spi, show crypto mib ipsec flowmib tunnel, show crypto mib isakmp flowmib failure, show crypto mib isakmp flowmib global, show crypto mib isakmp flowmib history, show crypto mib isakmp flowmib peer, show crypto mib isakmp flowmib tunnel, show tech-support ipsec.</p>

Glossary

peer--In the context of this module, a router or other device that participates in IPsec.

SA--security association. Description of how two or more entities use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. The transform and the shared secret keys are used for protecting the traffic.

transform--List of operations performed on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

tunnel--In the context of this module, a secure communication path between two peers, such as two routers. It does not refer to using IPsec in tunnel mode.



INDEX

- |
 - IPSec (IP Security) VPN monitoring **4, 8, 10**
 - additional references **8**
 - command reference **10**
 - IPSec (IP Security) VPN monitoring (*continued*)
 - restrictions **4**
 - IPsec and IKE MIB Support for Cisco VRF-Aware IPsec **14**
 - configuration examples **14**

