IPsec SNMP Support

Last Updated: October 17, 2011

The IPsec--SNMP Support feature can be used to learn the IPsec MIB feature version, enable and disable SNMP traps, and monitor and control the size of IPsec history tables.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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

"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."

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

- 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

Note CISCO-IPSEC-FLOW-MONITOR-MIB notifications are not supported before Cisco IOS Release 12.1(5a)E.

The CISCO-IPSEC-POLICY-MAP-MIB (ciscoIpSecPolMap) defines no notifications (the “IPSec Policy Map Notifications Group” is empty).

Information About IPsec-SNMP Support

IPsec-SNMP Support

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

VPN Device Manager

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.

See the VPN Device Manager Client for Cisco IOS Software (XSM Configuration) feature document for more information on Cisco VDM.

How to Configure IPsec-SNMP Support

Enabling IPsec SNMP Notifications

The following steps are used to enable a router to send IPsec trap or inform notifications to a specified host:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ipsec cryptomap** [**add** | **delete** | **attach**| **detach**]
4. Router(config)# **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.

	Command or Action	Purpose
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	Router(config)# **snmp-server enable traps isakmp**[**policy**{**add** | **delete**} | **tunnel**{**start** | **stop**}] **Example:** `Router(config)# snmp-server enable traps isakmp`	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 10.10.10.1 traps community1 ipsec`	Specifies the recipient of IPsec SNMP notification operations.

Configuring IPsec Failure History Table Size

Use the steps in this section to change the size of the failure history table. The default failure history table size is 200.

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.

	Command or Action	Purpose
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 50`	Changes the size of the IPsec failure history table.

Configuring IPsec Tunnel History Table Size

Follow the steps in this section to change the size of the tunnel history table. The default tunnel history table size is 200.

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 50`	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 commandto 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

Use the steps in this section to monitor the status of IPsec MIB information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show crypto mib ipsec flowmib history failure size**
4. **show crypto mib ipsec flowmib history tunnel size**
5. **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.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**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 4	**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 5	**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, page 7
- Specifying History Table Size Examples, page 8

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.cisco.com:

```
snmp-server host nms1.cisco.com public ipsec isakmp
Translating "nms1.cisco.com"...domain server (171.00.0.01) [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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
IPsec	Configuring Security for VPNs with IPsec
SNMP	*Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference*

MIBs

MIB	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR- MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	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

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 1 Feature Information for IPsec-SNMP Support

Feature Name	Releases	Feature Information
IPsec-SNMP Support	12.1(4)E 12.1(5a)E 12.2(4)T 12.2(8)T 12.1(11b)E 12.2(14)S	The IPsec--SNMP Support feature can be used to learn the IPsec MIB feature version, enable and disable SNMP traps, and monitor and control the size of IPsec history tables. This feature was introduced on the Cisco 7100, 7200, and 7500 series platforms in Cisco Release12.1(4)E. Support for CISCO-IPSEC-FLOW-MONITOR-MIB notifications was added in Cisco IOS Release 12.1(5a)E. This feature was integrated into Cisco IOS Release 12.2(4)T. In Cisco IOS Releases 12.2(8)T, 12.1(11b)E, the following commands were added to enable and disable IP Security (IPsec) MIB notifications: • **snmp-server enable traps ipsec** • **snmp-server enable traps isakmp** This feature was integrated into Cisco IOS Release 12.2(14)S. 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.**

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 (MIP). 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.

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