IPsec Diagnostics Enhancement

Last Updated: October 17, 2011

The Cisco IPsec Diagnostics Enhancement feature adds four sets of event statistics and an error history buffer to the Cisco IOS software for use in troubleshooting a virtual private network (VPN) that encrypts the data path.

Finding Feature Information

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

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

Prerequisites for the IPsec Diagnostics Enhancement

- You understand the IP security (IPsec) standard for network security.

Note Contact the Cisco Technical Assistance Center (TAC) before using this feature.

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

Restrictions for the IPsec Diagnostics Enhancement

- This feature and its commands are available only on Cisco IOS releases that support IPsec encryption.

Memory and Performance Impact

- This feature is enabled by default in the encryption data path and has a negligible impact on memory and performance.

Information About the IPsec Diagnostics Enhancement

Tracking Packet Processing Within a Switch or Router

Standard packet analyzers used for troubleshooting network issues capture packets between devices in the network but they cannot capture packet processing events inside a device, such as a router. Beginning with Cisco IOS Release 12.4(9)T, Cisco IOS software includes four sets of event statistics to track packet processing within a switch or router. These statistics help Cisco TAC engineers diagnose and resolve issues in encrypted networks. Each set of statistics tracks a different aspect of packet processing within a switch or router:

- Error counters track packet processing errors and associated packet drops. When a packet encounters an error, the first 64 bytes of that packet are stored in a buffer, to facilitate troubleshooting.
- Internal counters show the detailed movement of a packet, end to end, across an encryption data path.
- Punt counters track instances when the configured packet processing method failed, and an alternative method was used.
- Success counters record the data path checkpoints where packets are successfully forwarded.

You can view any one set of statistics, or all of them, or only those that have recorded errors. You must choose the display timeframe for the statistics.

How to Use the IPsec Diagnostics Enhancement

Note Contact the Cisco TAC before using this feature.

Displaying the Statistics

You can use the **show crypto datapath**command to display statistics that help troubleshoot an encrypted network.

SUMMARY STEPS

1. **enable**
2. **show crypto datapath {ipv4 | ipv6}** {**snapshot** | **realtime**} **{all | non-zero}**[**error** | **internal** | **punt** | **success**]

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 datapath {ipv4 | ipv6}** {**snapshot** | **realtime**} **{all | non-zero}**[**error** | **internal** | **punt** | **success**] **Example:** `Router# show crypto datapath snapshot success`	Displays the statistics from one or more specified counters. Use the keywords to specify the IP version used in the network (IPv4 or IPv6) and to specify whether to capture statistics in real time (**realtime**) or as of a single point in time (**snapshot**). You can also choose which statistics to display. The **all**keyword displays the output of all the counters, whether they have recorded events or not. The **non-zero**keyword displays only the output of counters that have recorded at least one event. Each of the other keywords displays one specific set of statistics, as described in the Information About the IPsec Diagnostics Enhancement, page 2.

Displaying the Error History

You can display the contents of the buffer that stores information from error events to diagnose the cause of errors. The **show monitor event-trace** command is updated with the **cfd**(crypto fault detection) keyword as a possible entry for the *component* argument to help with troubleshooting an encryption data path. Additional keywords allow you to specify the time span for which you want to display events. For example, you can display all events for the last 30 minutes.

For detailed information about the **show monitor event-trace** command, see the Master Command List.

SUMMARY STEPS

1. **enable**
2. **show monitor event-trace** [**all-traces**] [*component* **{ all | back** *time* **| clock** *time* **| from-boot** *seconds* **| latest | parameters }]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**show monitor event-trace** [**all-traces**] [*component* **{ all | back** *time* **| clock** *time* **| from-boot** *seconds* **| latest | parameters }]** **Example:** `Router# show monitor event-trace cfd all`	Displays the contents of the error trace buffer. - Use the keywords to specify which events to display and whether to display the trace file parameters.

Clearing the Counters or Error History

You can use the **clear crypto datapath** command to clear the counters or error history buffer in an encrypted network. Use the appropriate keywords to clear all counters or one specific counter.

SUMMARY STEPS

1. **enable**
2. **clear crypto datapath** {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**clear crypto datapath** {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**] **Example:** `Router# clear crypto datapath success`	Clears data for all counters or the specified counter.

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*
Configuring Security for VPNs with IPsec	Configuring Security for VPNs with IPsec

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

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 Diagnostics Enhancement

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 Diagnostics Enhancement

Feature Name	Releases	Feature Information
IPsec Diagnostics Enhancement	12.4(9)T	This feature adds four sets of event statistics and an error history buffer to the Cisco IOS software for use in troubleshooting a VPN that encrypts the data path The following commands were introduced or modified: **clear crypto datapath , show crypto datapath , show monitor event-trace**

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.