IPsec Diagnostics Enhancement

First Published: June 19, 2006
Last Updated: June 19, 2006

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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for the IPsec Diagnostics Enhancement" section on page 16.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

CISCO SYSTEMS

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

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.

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

To use the enhanced diagnostic tools for troubleshooting an encryption data path, you should understand the following concept:

- Tracking Packet Processing Within a Switch or Router, page 2

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, either **realtime**, which captures traffic statistics in real time, or **snapshot**, which captures statistics as of a single point in time.

How to Use the IPsec Diagnostics Enhancement

Note Contact the Cisco TAC before using this feature.

This section contains the following tasks:

- Displaying the Statistics, page 3 (optional)
- Displaying the Error History, page 4 (optional)
- Clearing the Counters or Error History, page 5 (optional)

Displaying the Statistics

You can use the **show crypto datapath** command to display statistics that help troubleshoot an encrypted network. 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" section on page 2.

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.

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, seethe *Cisco IOS Configuration Fundamentals Command Reference.*

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

The following sections provide references related to the IPsec Diagnostics Enhancement.

Related Documents

Related Topic	Document Title
Configuring Security for VPNs with IPsec	*Cisco IOS Security Configuration Guide*

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified.	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

RFCs

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

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **clear crypto datapath**
- **show crypto datapath**
- **show monitor event-trace**

clear crypto datapath

To clear the counters or error history buffers in an encrypted network, use the **clear crypto datapath** command in privileged EXEC mode.

clear crypto datapath {**ipv4** | **ipv6**} [**error** | **internal** | **punt** | **success**]

Syntax Description

ipv4	Clears all counters in a network using IPv4.
ipv6	Clears all counters in a network using IPv6.
error	(Optional) Clears the error history buffer.
internal	(Optional) Clears the internal event counter.
punt	(Optional) Clears the punt event counter.
success	(Optional) Clears the success event counter.

Command Default

All counters are cleared, unless a keyword is entered to specify one counter.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **clear crypto datapath** command to clear the history buffers or counters associated with an encrypted data path. You must specify the IP version for the network. If you only use the IP version keyword, all counters will be cleared. To clear only a specific counter, enter the keyword for that counter.

Examples

The following example shows how to clear all the counters in a network using IP version 4:

```
Router# clear crypto datapath ipv4
```

This example shows how to clear the success counter only:

```
Router# clear crypto datapath ipv4 success
```

Related Commands

Command	Description
show crypto datapath	Displays the counters associated with an encrypted data path.

show crypto datapath

To display the counters that help troubleshoot an encrypted data path, use the **show crypto datapath** command in privileged EXEC mode.

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

Syntax Description

ipv4	Designate IPv4 is used in the network.
ipv6	Designate IPv6 is used in the network.
realtime	Displays the counters that capture traffic statistics as they occur.
snapshot	Displays the counters that capture traffic statistics as of a single point in time.
all	Display all counters.
non-zero	Display all counters that have at least one event recorded.
error	(Optional) Display the packet processing and dropped packet errors.
internal	(Optional) Track the movement of a packet from end to end across an encrypted data path.
punt	(Optional) Display the instances when the configured processing method failed, and an alternative was used.
success	(Optional) Display the interfaces where packets were successfully processed.

Command Default

The command defaults are:

- IP version: **ipv4**
- Counters: **all**
- Display time: **realtime**

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **show crypto datapath counters** command to troubleshoot an encrypted data path.

Note Cisco recommends use of this command only for troubleshooting under the guidance of a Cisco TAC engineer.

You must specify the IP version used in the network. You can display all counters, only the counters that have recorded events, or one of these specific counters:

- 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 encrypted data path.
- Punt counters track instances when the configured packet processing method failed, and an alternative method was used. Because such instances might indicate a problem, it is useful to track them.
- Success counters help diagnose network performance problems. Frequently, although a network is configured for fast switching or CEF, packets are using a slower path. Success counters record the interfaces in the data path where packets were successfully processed and reveal the actual processing path.

You must also choose the display timeframe for the counters:

- The **realtime** option captures traffic statistics as they occur, and results in significant discrepancies between the first data reports and later data, because the counters increment with the traffic flow. This is the default option.
- The **snapshot** option captures traffic statistics as of a specific point in time, and results in a close match among all counts, because the counters do not increment with the continuing traffic flow.

Examples

The following example shows output from the **show crypto datapath** command. In this example, the **snapshot** option is specified for the timeframe, and only counters that have recorded events are displayed. The output of this command is intended for use by Cisco TAC engineers.

```
Router# show crypto datapath ipv4 snapshot non-zero

Success Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input core
    2nd round ok:            245      1st round ok:            118
  post crypto ip encrypt
    post encrypt ipflowok:   230
  crypto ceal post encrypt switch
    post encrypt ipflowok-2: 230
Error Statistics: Snapshot at 21:34:30 PST Mar 4 2006
Punt Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto ceal post decrypt switch
    fs to ps:                245
Internal Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input
    check input core not con 378      check input core consume 623

  crypto check input core
    came back from ce:       245      deny pak:                15

  crypto ipsec les fs
    not esp or ah:           1113
  post crypto ip decrypt
    decrypt switch:          245
  crypto decrypt ipsec sa check
    check ident success:     245
  crypto ceal post decrypt switch
    fs:                      245
  crypto ceal post decrypt fs
    les ip turbo fs:         245      tunnel ip les fs:        245
```

```
crypto ceal post decrypt ps
  proc inline:             245
crypto ceal punt to process inline
  coalesce:                245      simple enq:              245

crypto ceal post encrypt switch
  ps:                      230
crypto ceal post encrypt ps
  ps coalesce:             230      simple enq:              230

crypto engine ps vec
  ip encrypt:              230
crypto send epa packets
  ucast next hop:          230      ip ps send:              230
```

Related Commands

Command	Description
show monitor event-trace	Displays contents of error history buffers.

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** command in privileged EXEC configuration mode.

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

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. For a list of components that support event tracing in this release, use the **monitor event-trace ?** command.
all	Displays all event trace messages currently in memory for the specified component.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
time	Length of time in hours and minutes format (hh:mm).
clock	Displays event trace messages starting from a specific clock time.
time	Time from which to display messages in hours and minutes format (hh:mm).
from-boot	Displays event trace messages starting from a specified number of seconds after booting.
seconds	Number of seconds since the networking device was last booted (uptime). To view the uptime, in seconds, enter the **show monitor event-trace** *component* **from-boot ?** command.
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. The **spa** component keyword was added to support OIR event messages for shared port adapters (SPAs). The **bfd** keyword was added as a possible entry for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.0(31)S	Support for the **bfd** keyword was implemented in Cisco IOS Release 12.0(31)S.

Release	Modification
12.4(4)T	Support for the **bfd** keyword was implemented in Cisco IOS Release 12.4(4)T.
12.4(9)T	The **cfd** keyword was added as a possible entry for the *component* argument to display trace messages relating to crypto fault detection.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword will display the contents of the error trace buffers in an encryption data path.

Examples

Cisco IOS Releases 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

Use the **show monitor event-trace bfd all** command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
Router# show monitor event-trace bfd all

     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
            create, state Unknown -> Fail
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
            (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
            create, state Unknown -> Fail
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
             (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
            (from LC)
```

To view trace information for all components configured for event tracing on the networking device, enter the **show monitor event-trace all-traces** command. In this example, separate output is provided for each event and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789
```

```
Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

CFD Component for Cisco IOS Release 12.4(9)T

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all** command. In this example, events are shown separately, each beginning with a timestamp, followed by data from the error trace buffer. Cisco TAC engineers can use this information to diagnose the cause of the errors.

Note If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all

00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4

00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E

00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF

00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
        6BBD748F 87F5E253

00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6

00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

SPA Component Example

The following sample output illustrates the **show monitor event-trace** *component* **latest** command output for the **spa** component. The fields are self-explanatory.

```
Router# show monitor event-trace spa latest
00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idl
e
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idl
e
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idl
e
```

```
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  N
ew state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idl
e
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

Feature Information for the IPsec Diagnostics Enhancement

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for IPsec Diagnostics Enhancement

Feature Name	Releases	Feature Information
IPsec Diagnostics Enhancement	12.4(9)T	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.