



Crypto Conditional Debug Support

The Crypto Conditional Debug Support feature introduces three new command-line interfaces (CLIs) that allow users to debug an IP Security (IPSec) tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPSec operations and reducing the amount of debug output, users can better troubleshoot a router with a large number of tunnels.

Feature History for Crypto Conditional Debug Support

Feature History

Release	Modification
12.3(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Crypto Conditional Debug Support, page 2](#)
- [Restrictions for Crypto Conditional Debug Support, page 2](#)
- [Information About Crypto Conditional Debug Support, page 2](#)
- [How to Enable Crypto Conditional Debug Support, page 4](#)
- [Configuration Examples for the Crypto Conditional Debug CLIs, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



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

© 2003, 2009 Cisco Systems, Inc. All rights reserved.

Prerequisites for Crypto Conditional Debug Support

To use the new crypto CLIs, you must be using a crypto image such as the k8 or k9 subsystem.

Restrictions for Crypto Conditional Debug Support

- This feature does not support debug message filtering for hardware crypto engines.
- Although conditional debugging is useful for troubleshooting peer-specific or functionality related Internet Key Exchange (IKE) and IPSec problems, conditional debugging may not be able to define and check large numbers of debug conditions.
- Because extra space is needed to store the debug condition values, additional processing overhead is added to the CPU and memory usage is increased. Thus, enabling crypto conditional debugging on a router with heavy traffic should be used with caution.

Information About Crypto Conditional Debug Support

To enable the conditional crypto debug commands, you should understand the following concept:

- [Supported Condition Types, page 2](#)

Supported Condition Types

The new crypto conditional debug CLIs—[debug crypto condition](#), [debug crypto condition unmatched](#), and [show crypto debug-condition](#)—allow you to specify conditions (filter values) in which to generate and display debug messages related only to the specified conditions. [Table 1](#) lists the supported condition types.

Table 1 *Supported Condition Types for Crypto Debug CLI*

Condition Type (Keyword)	Description
connid ¹	An integer between 1–32766. Relevant debug messages will be shown if the current IPSec operation uses this value as the connection ID to interface with the crypto engine.
flowid ¹	An integer between 1–32766. Relevant debug messages will be shown if the current IPSec operation uses this value as the flow-ID to interface with the crypto engine.
FVRF	The name string of a virtual private network (VPN) routing and forwarding (VRF) instance. Relevant debug messages will be shown if the current IPSec operation uses this VRF instance as its front-door VRF (FVRF).

Table 1 Supported Condition Types for Crypto Debug CLI (continued)

Condition Type (Keyword)	Description
IVRF	The name string of a VRF instance. Relevant debug messages will be shown if the current IPSec operation uses this VRF instance as its inside VRF (IVRF).
peer group	A Unity group-name string. Relevant debug messages will be shown if the peer is using this group name as its identity.
peer hostname	A fully qualified domain name (FQDN) string. Relevant debug messages will be shown if the peer is using this string as its identity; for example, if the peer is enabling IKE Xauth with this FQDN string.
peer ipaddress	A single IP address. Relevant debug messages will be shown if the current IPSec operation is related to the IP address of this peer.
peer subnet	A subnet and a subnet mask that specify a range of peer IP addresses. Relevant debug messages will be shown if the IP address of the current IPSec peer falls into the specified subnet range.
peer username	A username string. Relevant debug messages will be shown if the peer is using this username as its identity; for example, if the peer is enabling IKE Extended Authentication (Xauth) with this username.
SPI ¹	A 32-bit unsigned integer. Relevant debug messages will be shown if the current IPSec operation uses this value as the SPI.

1. If an IPSec connid, flowid, or SPI is used as a debug condition, the debug messages for a related IPSec flow are generated. An IPSec flow has two connids, flowids, and SPIs—one inbound and one outbound. Both two connids, flowids, and SPIs can be used as the debug condition that triggers debug messages for the IPSec flow.

How to Enable Crypto Conditional Debug Support

This section contains the following procedures:

- [Enabling Crypto Conditional Debug Messages, page 4](#)
- [Enabling Crypto Error Debug Messages, page 6](#)

Enabling Crypto Conditional Debug Messages

To enable crypto conditional debug filtering, you must perform the following tasks.

Performance Considerations

- Before enabling crypto conditional debugging, you must decide what debug condition types (also known as debug filters) and values will be used. The volume of debug messages is dependent on the number of conditions you define.



Note Specifying numerous debug conditions may consume CPU cycles and negatively affect router performance.

- Your router will perform conditional debugging only after at least one of the global crypto debug commands—**debug crypto isakmp**, **debug crypto ipsec**, and **debug crypto engine**—has been enabled. This requirement helps to ensure that the performance of the router will not be impacted when conditional debugging is not being used.

Disable Crypto Debug Conditions

If you choose to disable crypto conditional debugging, you must first disable any crypto global debug CLIs you have issued; thereafter, you can disable conditional debugging.



Note The **reset** keyword can be used to disable all configured conditions at one time.

SUMMARY STEPS

1. **enable**
2. **debug crypto condition** [*connid integer engine-id integer*] [*flowid integer engine-id integer*] [*fvrif string*] [*ivrf string*] [*peer [group string] [hostname string] [ipv4 ipaddress] [subnet subnet mask] [username string]*] [*spi integer*] [**reset**]
3. **show crypto debug-condition** {[*peer*] [*connid*] [*spi*] [*fvrif*] [*ivrf*] [*unmatched*]}
4. **debug crypto isakmp**
5. **debug crypto ipsec**
6. **debug crypto engine**
7. **debug crypto condition unmatched** [*isakmp | ipsec | engine*] (optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>debug crypto condition [connid <i>integer</i>] [engine-id <i>integer</i>] [flowid <i>integer</i>] [engine-id <i>integer</i>] [fvrf <i>string</i>] [ivrf <i>string</i>] [peer [group <i>string</i>] [hostname <i>string</i>] [ipv4 <i>ipaddress</i>] [subnet <i>subnet mask</i>] [username <i>string</i>]] [spi <i>integer</i>] [reset]</p> <p>Example: Router# debug crypto condition connid 2000 engine-id 1</p>	<p>Defines conditional debug filters.</p>
Step 3	<p>show crypto debug-condition {[peer] [connid] [spi] [fvrf] [ivrf] [unmatched]}</p> <p>Example: Router# show crypto debug-condition spi</p>	<p>Displays crypto debug conditions that have already been enabled in the router.</p>
Step 4	<p>debug crypto isakmp</p> <p>Example: Router# debug crypto isakmp</p>	<p>Enables global IKE debugging.</p>
Step 5	<p>debug crypto ipsec</p> <p>Example: Router# debug crypto ipsec</p>	<p>Enables global IPsec debugging.</p>
Step 6	<p>debug crypto engine</p> <p>Example: Router# debug crypto engine</p>	<p>Enables global crypto engine debugging.</p>
Step 7	<p>debug crypto condition unmatched [isakmp ipsec engine]</p> <p>Example: Router# debug crypto condition unmatched ipsec</p>	<p>(Optional) Displays debug conditional crypto messages when no context information is available to check against debug conditions.</p> <p>If none of the optional keywords are specified, all crypto-related information will be shown.</p>

Enabling Crypto Error Debug Messages

To enable crypto error debug messages, you must perform the following tasks.

debug crypto error CLI

Enabling the **debug crypto error** command displays only error-related debug messages, thereby, allowing you to easily determine why a crypto operation, such as an IKE negotiation, has failed within your system.



Note

When enabling this command, ensure that global crypto debug commands are not enabled; otherwise, the global commands will override any possible error-related debug messages.

SUMMARY STEPS

1. **enable**
2. **debug crypto {isakmp | ipsec | engine} error**

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	debug crypto {isakmp ipsec engine} error Example: Router# debug crypto ipsec error	Enables only error debugging messages for a crypto area.

Configuration Examples for the Crypto Conditional Debug CLIs

This section includes the following examples:

- [Enabling Crypto Conditional Debugging: Example, page 7](#)
- [Disabling Crypto Conditional Debugging: Example, page 7](#)

Enabling Crypto Conditional Debugging: Example

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3, and when the connection-ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router# debug crypto condition connid 2000 engine-id 1
Router# debug crypto condition peer ipv4 10.1.1.1
Router# debug crypto condition peer ipv4 10.1.1.2
Router# debug crypto condition peer ipv4 10.1.1.3
Router# debug crypto condition unmatched
! Verify crypto conditional settings.
Router# show crypto debug-condition
```

```
Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON
```

```
IKE peer IP address filters:
10.1.1.1 10.1.1.2 10.1.1.3
```

```
Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
```

```
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
```

Disabling Crypto Conditional Debugging: Example

The following example shows how to disable all crypto conditional settings and verify that those settings have been disabled:

```
Router# debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router# show crypto debug-condition
```

```
Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Additional References

The following sections provide references to the Crypto Conditional Debug Support feature.

Related Documents

Related Topic	Document Title
IPSec and IKE configuration tasks	“Internet Key Exchange for IPsec VPNs” section of <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
IPSec and IKE commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

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

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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

The following commands are introduced or modified in the feature or features

- **debug crypto condition**
- **debug crypto condition unmatched**
- **debug crypto error**
- **show crypto debug-condition**

For information about these commands, see the *Cisco IOS Security Command Reference* at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

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.

© 2003–2010 Cisco Systems, Inc. All rights reserved.

