Option to Disable Hardware Crypto EngineFailover to Software Crypto Engine

Last Updated: October 20, 2011

The Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine feature gives you the option of configurirng your router so that failover to the software crypto engine does not occur even if the hardware crypto engine fails.

Feature History for Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

Release	Modification
12.3(14)T	This feature was introduced.

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.

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

Prerequisites for Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

- You must have the Cisco IOS IP Security (IPSec) framework configured on your network.

Information About Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

- Hardware Crypto Engine Failover to the Software Crypto Engine Overview, page 2
- Option to Disable Hardware Crypto Engine Failover, page 2

Hardware Crypto Engine Failover to the Software Crypto Engine Overview

Cisco IOS IPSec traffic can be supported both by a hardware encryption engine and by a software crypto engine (that is, by the main CPU, which is running a software encryption algorithm). If the hardware encryption engine fails, the software on the main CPU attempts to perform the IPSec functions. However, the main CPU software routines have only a small percentage of bandwidth compared with those of the hardware encryption engine. If a sufficient amount of traffic is being handled by the hardware engine, it is possible that on failover, the main CPU may try to handle more traffic than it can, causing the router to fail.

Option to Disable Hardware Crypto Engine Failover

The Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine feature allows you to configure your router so that the hardware crypto engine does not automatically fail over to the software crypto engine.

For situations in which you prefer that the software routines on the main CPU handle the hardware crypto engine failover, the default is that failover does occur.

How to Configure Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

- Disabling Hardware Crypto Engine Failover to the Software Crypto Engine, page 2

Disabling Hardware Crypto Engine Failover to the Software Crypto Engine

To disable hardware crypto engine failover to the software crypto engine, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto engine software 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	**no crypto engine software ipsec** **Example:** `Router (config)# no crypto engine software ipsec`	Disables hardware crypto engine failover to the software crypto engine. • To reenable failover, use the **crypto engine software ipsec**form of this command.

Configuration Examples for Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

- Disabled Hardware Crypto Engine Failover Example, page 3

Disabled Hardware Crypto Engine Failover Example

The following example shows that hardware crypto engine failover to the software crypto engine has been disabled:

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
boot-end-marker
!
```

```
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
no crypto engine software ipsec
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 209.165.201.2!
!
crypto ipsec transform-set basic esp-des esp-md5-hmac!
crypto map mymap 10 ipsec-isakmp
 set peer 209.165.201.2
 set transform-set basic
 match address 101
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 209.165.200.2 255.255.255.252 serial restart-delay 0 crypto map mymap!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101
remark Crypto ACL!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Additional References

The following sections provide references related to Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine.

Related Documents

Related Topic	Document Title
Cisco IOS Security commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing 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 existing MIBs has not been modified by this feature.	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
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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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.	http://www.cisco.com/techsupport

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.