



Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

The Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine feature gives you the option of configuring 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 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://www.cisco.com/go/fn>. 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 Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine, page 2](#)
- [Information About Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine, page 2](#)
- [How to Configure Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine, page 2](#)
- [Configuration Examples for Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine, page 3](#)
- [Additional References, page 5](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

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

To configure the Disable Hardware Crypto Engine Failover to Software Crypto Engine feature, you should understand the following concepts:

- [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

This section contains the following procedure:

- [Disabling Hardware Crypto Engine Failover to the Software Crypto Engine, page 3](#)

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	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>no crypto engine software ipsec</code> Example: Router (config)# <code>no crypto engine software ipsec</code>	Disables hardware crypto engine failover to the software crypto engine. <ul style="list-style-type: none"> • To reenable failover, use the <code>crypto engine software ipsec</code> form of this command.

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

This section includes the following configuration example:

- [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	<i>Cisco IOS Security Command Reference</i> , Release 12.3T

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 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
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/public/support/tac/home.shtml

Command Reference

This section documents the following new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

- [no crypto engine software ipsec](#)

no crypto engine software ipsec

To disable hardware crypto engine failover to the software crypto engine, use the **no crypto engine software ipsec** command in global configuration mode. To reenable failover, use the **crypto engine software ipsec** form of this command.

no crypto engine software ipsec

crypto engine software ipsec

Syntax Description This command has no arguments or keywords.

Defaults Failover is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1E	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines Use this command for those situations in which the amount of IP Security (IPSec) traffic is more than can be handled (because of bandwidth) by the software routines on the CPU.

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

```
no crypto engine software ipsec
```

The following example shows that hardware crypto engine failover has been reenabled:

```
crypto engine software ipsec
```

Related Commands	Command	Description
	crypto engine accelerator	Enables the onboard hardware accelerator of the router for IPSec encryption.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. 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. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.