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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

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 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 4
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 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>no crypto engine software ipsec</td>
<td>Disables hardware crypto engine failover to the software crypto engine.</td>
</tr>
<tr>
<td></td>
<td>• To reenable failover, use the crypto engine software ipsec form of this command.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
The following commands are introduced or modified in the feature or features

- **no crypto engine software ipsec**


For information about all Cisco IOS commands, see the Command Lookup Tool at [http://tools.cisco.com/Support/CLILookup](http://tools.cisco.com/Support/CLILookup) or the Master Command List.