



Virtual Private Network Configuration for the Cisco 1700 Routers

This feature module describes the Virtual Private Network (VPN) feature for Cisco 1720 and Cisco 1750 routers. It describes the benefits of the new feature, supported platforms, configuration, related documents, and provides command reference information.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Prerequisites, page 3
- Configuring Encryption and Decryption Acceleration, page 3
- Configuration Examples, page 3
- Command Reference, page 4
- Debug Commands, page 4

Feature Overview

The Cisco 1700 series routers, which includes the Cisco 1720 and 1750 models, are modular access routers for small and medium businesses and small branch offices. Cisco 1700 routers deliver routing, firewall, and VPN functions for Internet data and voice applications.

The VPN module, which fits into a slot inside the Cisco 1720 or 1750 chassis, assists the host processor by accelerating layer 3 IP Security (IPSec) data and voice encryption and decryption. The VPN module supports DES and 3DES encryption algorithms, MD5 and SHA-1 hashing, and Diffie-Hellman key generation.

The VPN module encrypts data using DES and 3DES algorithms at speeds suitable for full duplex T1/E1 serial connections (4 megabits per second for 1518-byte packets). Equipped with a VPN module, a Cisco 1700 router supports up to 100 encrypted tunnels for concurrent sessions with mobile users or other sites.

Benefits

- Accelerates DES and 3DES data encryption and decryption and MD5 and SHA data authentication up to 4 Mbps (1518-byte packets)
- Delivers up to 100 concurrent secure sessions (IPSec tunnels)
- Supports RSA and Diffie Hellman algorithms for IKE and ISAKMP key generation and exchange
- With all the above features, optimizes Cisco 1720 and 1750 routers for Virtual Private Networks (VPNs)

Restrictions

- Export Regulations on the VPN Module: DES and 3DES software for the VPN Module is controlled by US export regulations on encryption products. The module itself is not controlled. Unites States regulations require the recording of names and addresses of recipients of DES and 3DES software. The Cisco ordering process for DES and 3DES software enforces these requirements. For details, see <http://www.cisco.com/wwl/export/crypto/>.
- Do not use Cisco express forwarding (CEF) switching if a VPN module is installed in a Cisco 1700 series router.
- Refer to the *Caveats for Cisco IOS Release 12.1 T* document and the *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.1(1)XC* for known and unresolved caveats common to hardware encryption or IPSec functionality.

Related Features and Technologies

- IPSec uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network. Cisco provides full Encapsulating Security Payload (ESP) and Authentication Header (AH) support.
- The Internet Key Exchange (IKE), formerly known as the Internet Security Association Key Management Protocol or ISAKMP/Oakley, provides security association management. The IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys.
- Other hardware encryption module features: Cisco 7000 series routers support an Integrated Service Adapter (ISA).

Related Documents

- *Installing the Cisco 1700 Series Encryption Module*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.1(1)XC*
- *Caveats for Cisco IOS Release 12.1 T*
- *Cisco 1700 Router Software Configuration Guide*
- *Cisco 1720 Router Hardware Installation Guide*

Supported Platforms

- Cisco 1720
- Cisco 1750

Prerequisites

Before you can enable the VPN feature on Cisco 1720 or Cisco 1750 routers, the VPN module must be installed and running one of the following Cisco IOS images with IPSec functionality:

- c1700-sy56i-mz
- c1700-o3sy56i-mz
- c1700-k2sy-mz
- c1700-k2o3sy-mz
- c1700-bno3r2sy56i-mz
- c1700-bk2no3r2sy-mz
- c1700-sv3y56i-mz
- c1700-o3sv3y56i-mz
- c1700-k2sv3y-mz
- c1700-k2o3sv3y-mz
- c1700-bno3r2sv3y56i-mz
- c1700-bk2no3r2sv3y-mz

Configuring Encryption and Decryption Acceleration

There are no specific configuration commands. All the commands listed in this document are for Cisco Systems Technical Assistance Center (TAC) debugging purposes only.

Configuration Examples

See the “Examples” headings in the section “Command Reference” for samples of the commands **show crypto engine accelerator sa-database**, **debug crypto engine accelerator logs**, and **show crypto engine accelerator logs**.

Command Reference

This section describes in detail the new Cisco IOS debugging commands for the VPN module on Cisco 1700 series routers. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **debug crypto engine accelerator logs**
- **show crypto engine accelerator logs**
- **show crypto engine accelerator sa-database**

Debug Commands

This section documents the new **debug** commands related to the VPN module on Cisco 1700 series routers.

debug crypto engine accelerator logs

To enable logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag, use the privileged mode **debug crypto engine accelerator logs** command.

debug crypto engine accelerator logs

no debug crypto engine accelerator logs

Syntax Description This command contains no arguments or keywords.

Defaults The logging of commands sent from the VPN module driver to the VPN module hardware is disabled.

Command Modes Privileged.

Command History

Release	Modification
Cisco IOS Release 12.1(1)XC	The command debug crypto engine accelerator logs was introduced on the Cisco 1720 and Cisco 1750 routers.

Usage Guidelines The command **debug crypto engine accelerator logs** is intended for Cisco Systems TAC personnel only to collect debugging information. Use the command when encryption traffic is sent to the router and a problem with the encryption module is suspected.

Examples

The command **debug crypto engine accelerator logs** uses a debug flag to log commands and associated parameters sent from the VPN module driver to the VPN module hardware as follows:

```
router# debug crypto engine accelerator logs
encryption module logs debugging is on
```

Related Commands

Command	Description
debug crypto engine accelerator control [detail]	For nondetail mode, print each control command and length. For detail mode, print the request and response descriptor contents.
debug crypto engine accelerator packet [detail] [number <i>n</i>] [length <i>l</i>]	For nondetail mode, print whether the packet is for encryption and decryption and the packet data (that is, the number <i>n</i> of packets before debugging automatically stops and the number of bytes [length <i>l</i>] of the packet to print). For detail mode, print additional debug information related to packet processing by the encryption engine accelerator.
crypto engine accelerator	This command enables or disables the crypto engine accelerator if it exists. On all platforms crypto engine accelerator is the default. ¹
show crypto engine accelerator logs	Print information about the last 32 CryptoGraphics eXtensions (CGX) Library, packet processing commands, and associated parameters sent from the VPN module driver to the VPN module hardware.
show crypto engine accelerator ring control	Print out the contents of the encryption engine accelerator control command ring(s). ¹
show crypto engine accelerator ring packet	Print out the contents of the encryption engine accelerator input and output packet rings. ¹
show crypto engine accelerator sa-database	Print active (in-use) entries in the platform-specific VPN module database.
show crypto engine accelerator statistic	Print out the statistics (input and output packets and various error counters) for the encryption engine accelerator. ¹
show crypto engine configuration	Print out the version and other related information on the encryption engine.

1. Note that on the Cisco 1700 series platform, the argument [slot] for the command is not relevant because there can only be one VPN module.

show crypto engine accelerator logs

To print information about the last 32 CryptoGraphics eXtensions (CGX) Library, packet processing commands, and associated parameters sent from the VPN module driver to the VPN module hardware, use the privileged mode **show crypto engine accelerator logs** command.

show crypto engine accelerator logs

Syntax Description This command contains no arguments or keywords.

Command Modes Privileged.

Command History

Release	Modification
Cisco IOS Release 12.1(1)XC	The command show crypto engine accelerator logs was introduced on the Cisco 1720 and Cisco 1750 routers.

Usage Guidelines The command **show crypto engine accelerator logs** is intended for Cisco Systems TAC personnel only to collect debugging information. Use the command when encryption traffic is sent to the router and a problem with the encryption module is suspected. Use the command **debug crypto engine accelerator logs** to enable command logging before using the command **show crypto engine accelerator logs**.

Examples

```
router# show crypto engine accelerator logs
Contents of packet log (current index = 20):

tag = 0x5B02, cmd = 0x5000
param[0] = 0x000E, param[1] = 0x57E8
param[2] = 0x0008, param[3] = 0x0000
param[4] = 0x0078, param[5] = 0x0004
param[6] = 0x142C, param[7] = 0x142C
param[8] = 0x0078, param[9] = 0x000C
tag = 0x5B03, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x583C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
```

```
tag = 0x5C00, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x57BC
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
```

•
•
•

```
tag = 0x5A01, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x593C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
```

Contents of cgx log (current index = 12):

```
cmd = 0x0074 ret = 0x0000
param[0] = 0x0010, param[1] = 0x028E
param[2] = 0x0039, param[3] = 0x0D1E
param[4] = 0x0100, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0062 ret = 0x0000
param[0] = 0x0035, param[1] = 0x1BE0
param[2] = 0x0100, param[3] = 0x0222
param[4] = 0x0258, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0063 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0000, param[3] = 0x0000
param[4] = 0x0000, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x020A
param[8] = 0x002D, param[9] = 0x0000
```

•
•
•

```
cmd = 0x0065 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0010, param[3] = 0x028E
param[4] = 0x00A0, param[5] = 0x0008
param[6] = 0x0001, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
```

Related Commands

Command	Description
debug crypto engine accelerator control [detail]	For nondetail mode, print each control command and length. For detail mode, print the request and response descriptor contents.
debug crypto engine accelerator logs	Enable logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.
debug crypto engine accelerator packet [detail] [number <i>n</i>] [length <i>l</i>]	For nondetail mode, print whether the packet is for encryption and decryption and the packet data (that is, the number <i>n</i> of packets before debugging automatically stops and the number of bytes [length <i>l</i>] of the packet to print). For detail mode, print additional debug information related to packet processing by the encryption engine accelerator.
crypto engine accelerator	This command enables or disables the crypto engine accelerator if it exists. On all platforms crypto engine accelerator is the default. ¹
show crypto engine accelerator ring control	Print out the contents of the encryption engine accelerator control command ring(s). ¹
show crypto engine accelerator ring packet	Print out the contents of the encryption engine accelerator input and output packet rings. ¹
show crypto engine accelerator sa-database	Print active (in-use) entries in the platform-specific VPN module database.
show crypto engine accelerator statistic	Print out the statistics (input and output packets and various error counters) for the encryption engine accelerator. ¹
show crypto engine configuration	Print out the version and other related information on the encryption engine.

1. Note that on the Cisco 1700 series platform, the argument [slot] for the command is not relevant because there can only be one VPN module.

show crypto engine accelerator sa-database

To print active (in-use) entries in the platform-specific VPN module database, use the privileged mode **show crypto engine accelerator sa-database** command.

show crypto engine accelerator sa-database

Syntax Description This command contains no arguments or keywords.

Command Modes Privileged.

Command History

Release	Modification
Cisco IOS Release 12.1(1)XC	The command show crypto engine accelerator sa-database was introduced on the Cisco 1720 and Cisco 1750 routers.

Usage Guidelines The command **show crypto engine accelerator sa-database** is intended for Cisco Systems TAC personnel only to collect debugging information. Use the command when encryption traffic is sent to the router and a problem with the encryption module is suspected.

Examples

```
router# show crypto engine accelerator sa-database
Flow Summary
  Index  Algorithms
  005    tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
  006    tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
  007    tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
  008    tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
  009    tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
  010    tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
SA Summary:
  Index  DH-Index  Algorithms
  003    001(deleted)  DES SHA
  004    002(deleted)  DES SHA
DH Summary
  Index Group Config
```

Related Commands

Command	Description
debug crypto engine accelerator control [detail]	For nondetail mode, print each control command and length. For detail mode, print the request and response descriptor contents.
debug crypto engine accelerator logs	Enable logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.
debug crypto engine accelerator packet [detail] [number <i>n</i>] [length <i>l</i>]	For nondetail mode, print whether the packet is for encryption and decryption and the packet data (that is, the number <i>n</i> of packets before debugging automatically stops and the number of bytes [length <i>l</i>] of the packet to print). For detail mode, print additional debug information related to packet processing by the encryption engine accelerator.
crypto engine accelerator	This command enables or disables the crypto engine accelerator if it exists. On all platforms crypto engine accelerator is the default. ¹
show crypto engine accelerator logs	Print information about the last 32 CryptoGraphics eXtensions (CGX) Library, packet processing commands, and associated parameters sent from the VPN module driver to the VPN module hardware.
show crypto engine accelerator ring control	Print out the contents of the encryption engine accelerator control command ring(s). ¹
show crypto engine accelerator ring packet	Print out the contents of the encryption engine accelerator input and output packet rings. ¹
show crypto engine accelerator statistic	Print out the statistics (input and output packets and various error counters) for the encryption engine accelerator. ¹
show crypto engine configuration	Print out the version and other related information on the encryption engine.

1. Note that on the Cisco 1700 series platform, the argument [slot] for the command is not relevant because there can only be one VPN module.