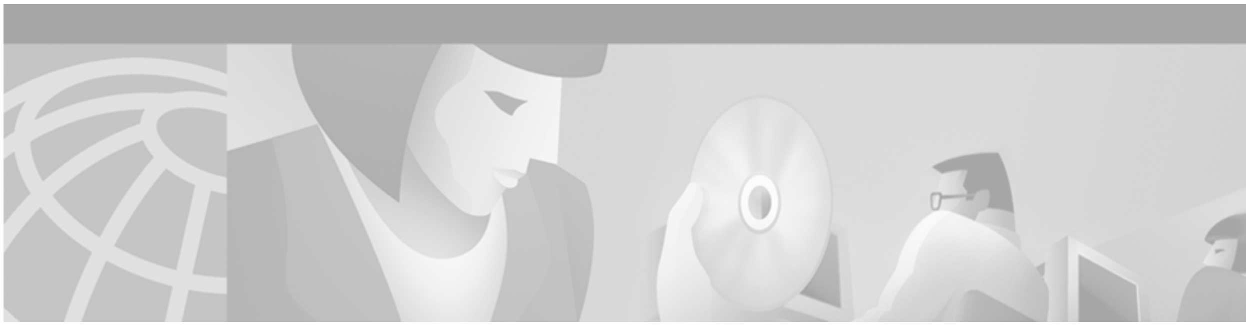


# Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS IPSec

**July 2002 (version 1.0)**

## Contents

This document describes how to install and configure Cisco IOS routers in accordance with the Common Criteria Evaluation Assurance Level 4 (EAL4) evaluated Cisco IOS IP Security (IPSec).

**Note** Any changes to the information provided in this document will result in noncompliance between the Cisco IOS router and the Cisco IOS IPSec evaluation and may make the router insecure.

This document includes the following sections:

Cisco Systems

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

# Introduction

This document is an addendum to the Cisco IOS Release 12.1 and Release 12.2 documentation sets, which should be read prior to configuring a Cisco IOS router in accordance with the Common Criteria EAL4 evaluated Cisco IOS IPSec.

The Cisco IOS Release 12.1 and Release 12.2 documentation sets include the following elements:

- Configuration guides, which provide a descriptive overview of functions, the commands needed to enable specified functions, and the sequence of operations that should be followed to implement them.
- Command references, which provide a complete description of all configuration commands and options, their effects, and examples and guidelines for the use of the commands. The command references should be used to confirm detailed syntax and functionality options.
- System Error Messages, which describe all error messages issued by Cisco IOS routers.

This document references the following Cisco IOS Release 12.1 and Release 12.2 documentation:

- *Cisco IOS Configuration Fundamentals Configuration Guide*
- *Cisco IOS Configuration Fundamentals Command Reference*
- *Cisco IOS Security Configuration Guide*
- *Cisco IOS Security Command Reference*
- *Cisco IOS IP Configuration Guide*
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*
- *Cisco IOS System Error Messages*
- Release Notes and Caveats for Cisco IOS Release 12.2

Cisco IOS documentation is available on CD-ROM, in printed paper form, and online (in HTML and PDF formats). This document should be used in conjunction with the October 2001 edition of the CD-ROM–based documentation.

# Audience

This document is written for administrators who configure Cisco IOS routers in accordance with the Common Criteria evaluated Cisco IOS IPSec. This document assumes that you are familiar with networks and networking technology, are a trusted individual, and been trained to use the IPSec technology and its applications, such as site-to-site Virtual Private Networks (VPNs). There are no components of the Cisco IOS IPSec that are accessible to nonadministrative users (end users); therefore, there is not any user-level documentation.

# Supported Hardware and Software

The hardware and software combinations that are complaint with Common Criteria evaluated Cisco IOS IPSec are outlined in Table 1. (The supporting hardware documentation is outlined in Table 2.)

**Note** Only the hardware versions of the IPSec VPN hardware modules that are listed in Table 8 are compliant with Common Criteria evaluated Cisco IOS IPSec. To display the hardware version of an IPSec VPN hardware module, use the **show diag** command in privileged EXEC mode.

*Table 1 Supported Hardware and Software for the Common Criteria Evaluated Cisco IOS IPSec*

| Hardware Family | Supported Models | Optional IPSec VPN Hardware Module | Software Versions | Software Feature |
|---|---|---|---|---|
| Cisco 1700 series | 1720, 1750 | MOD1700-VPN | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| Cisco 2600 series | 2610, 2611, 2612, 2613, 2620, 2621, 2650, and 2651 | AIM-VPN/BP | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| Cisco 3600 series | 3620, 3640 | NM-VPN/MP | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| | 3660 | AIM-VPN/HP | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| Cisco 7100 series[2] | 7120, 7140 | SA-ISA or SM-ISM | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| | | SM-VAM[3] or SA-VAM[3] | Cisco IOS 12.1(10)E | IPSec 56<br>IPSec 3DES[1] |
| Cisco 7200 series | 7204, 7206, 7204VXR, 7206VXR | SA-ISA (max 2) | Cisco IOS 12.2(6) | IPSec 56<br>IPSec 3DES[1] |
| | | SA-VAM[3] | Cisco IOS 12.1(10)E | IPSec 56<br>IPSec 3DES[1] |

[1] The Cisco IOS software image must contain at least the IPSec 56 or IPSec 3DES feature, which can be in combination with other feature sets such as IP, Firewall, Plus, or Enterprise.

[2] The Cisco 7100 series and Cisco 7200 series without optional IPSec hardware acceleration modules can be configured with Cisco IOS Release 12.2(6)T or Cisco IOS Release 12.1(10)E.

[3] Cisco 7100 series and Cisco 7200 series that are equipped with an SA-VAM or SM-VAM do not support Rivest, Shamir, and Adelman (RSA) public or private key pairs for IKE authentication.

# Security Information

This section contains the following sections:

- Supported Hardware Documentation
- Organizational Security Policy
- Security Implementation Considerations

## Supported Hardware Documentation

In addition to the regulatory compliance documentation for each hardware platform listed in Table 2, the sections that follow provide additional security information for use with a Common Criteria evaluation Cisco IOS IPSec router.

***Table 2 Regulatory Compliance and Safety Information Documentation for Common Criteria Evaluated Cisco IOS IPSec Hardware Platforms***

| Hardware Family | Regulatory Compliance and Safety Information Documentation |
|---|---|
| Cisco 1700 series | *Regulatory Compliance and Safety Information for Cisco 1700 Series Routers* |
| Cisco 2600 series | *Regulatory Compliance and Safety Information for the Cisco 2600 Series Routers* |
| Cisco 3600 series | *Regulatory Compliance and Safety Information for the Cisco 3600 Series Routers* |
| Cisco 7100 series | *Regulatory Compliance and Safety Information for Cisco 7100 Series VPN Routers* |
| Cisco 7200 series | *Regulatory Compliance and Safety Information for Cisco 7200 Series Routers* |

## Organizational Security Policy

Ensure that your Cisco IOS router is delivered, installed, managed, and operated in a manner that maintains an organizational security policy for IPSec protected traffic. The organizational security policy *must* describe the following variables:

- The networks that are to be considered trusted and untrusted
- The traffic flows between trusted networks that must be protected using IPSec to provide confidentiality, authenticity, and integrity in terms of source and destination IP addresses or port number
- The Cisco IOS routers that are associated with each trusted network that provide IPSec services to the identified traffic flows

The administrator must identify which interfaces on the Cisco IOS router are considered trusted and untrusted. An untrusted interface is one that is connected to an untrusted network over which the administrator wishes to send and receive trusted traffic that is protected by IPSec encryption.

*Figure 1 Organizational Security Policy Example*

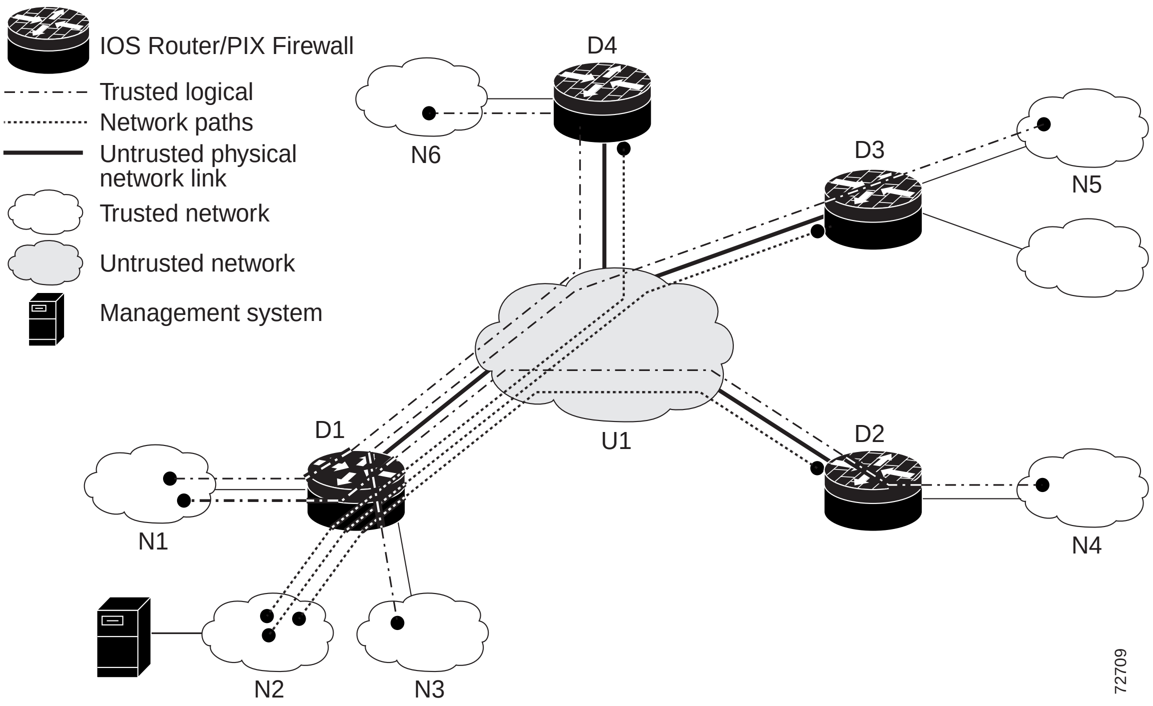


Figure 1 displays an organizational security policy with traffic flows that are identified solely by source and destination IP addresses. All Cisco IOS routers (D1, D2, D3, and D4) must be configured to implement a portion of the organizational security policy. For example, Router D1 has three trusted networks attached to it (N1, N2, and N3); this router implements a policy for the three trusted network-to-network flows and three secure management flows that cross the untrusted network (U1). (The policy that Router D1 implements is outlined in Table 3.)

*Table 3 Policy for Cisco IPSec Crypto System Example*

| Source | Destination | Peer Device |
|---|---|---|
| N1 | N6 | D4 |
| N1 | N5 | D3 |
| N3 | N4 | D2 |
| N2 | D2 | D2 |
| N2 | D3 | D3 |
| N2 | D4 | D4 |

All other routers (D2, D3, D4) must have a matching configuration to implement the organizational security policy. Each of the rows in Table 3 is configured on the Cisco IOS router as an IPSec tunnel.

An organizational security policy may implement a site-to-site VPN between multiple locations (trusted networks) over the Internet (an untrusted network), or it may specify that all LAN traffic (trusted networks) be encrypted when transmitted over any WAN link (untrusted network).

# Security Implementation Considerations

The following sections provide implementation considerations that need to be addressed to administer Cisco IOS routers in a secure manner that is consistent with Common Criteria evaluated Cisco IOS IPSec:

- Evaluated Configuration
- Physical Security
- Certificate Authority
- Time Sources
- Access Control
- Remote Administration and Management
- SNMP
- Logging and Messages
- Access Lists
- Monitoring and Maintenance

## Evaluated Configuration

Only the hardware and software version combinations that are described in Table 1 can be used to implement an evaluated configuration. You will invalidate the evaluated status of a particular hardware platform if you change the software to a different version.

The Common Criteria Target of Evaluation (TOE) for Cisco IOS IPSec defines only the following features:

- IPSec Internet Key Exchange (IKE) using preshared keys, RSA keys, or digital certificates

**Note** The Cisco 7100 series and Cisco 7200 series with an SM-VAM or SA-VAM do not support IKE with RSA keys.

- IPSec encapsulating security payload (ESP) using tunnel mode with Data Encryption Standard (DES) or 3DES
- Optional hardware acceleration of IPSec (as specified in Table 1)
- Cryptographic key generation and management
- Inbound access lists
- Message logging
- User authentication for access to the command-line interface (CLI) using locally configured passwords

**Note** Although Cisco IOS supports authentication, authorization, and accounting (AAA) user authentication, it is not supported within the Cisco IOS-IPSec TOE.

- Time management

All other hardware and software features and functions of a Cisco IOS router are outside the scope of this evaluated product configuration, and therefore can be used in conjunction with the TOE functions only if the TOE functions are configured, operated, and managed in accordance with this document.

To ensure that the Cisco IOS router configuration continues to meet the organizational security policy, you should review your router configurations for the following possible changes:

- Changes in the Cisco IOS router configuration
- Changes in the organizational security policy
- Changes in the threats presented from untrusted networks
- Changes in the administration and operation staff or of the physical environment of the Cisco IOS router

## Physical Security

The Cisco IOS router must be located in a physically secure environment in which only a trusted administrator has access. The secure configuration of a Cisco IOS router can be compromised if an intruder gains physical access to the router.

## Certificate Authority

If digital certificates are used to provide authentication between evaluated Cisco IOS IPSec routers, the certificate authority that issues the certificates must be trusted or evaluated to the same level as Cisco IOS IPSec (Common Criteria EAL4).

## Time Sources

Routers configured in accordance with the Cisco IOS IPSec evaluation must time-stamp system log messages. For Cisco routers without internal, real-time hardware clocks (Cisco 1700, 2600, 3600 series), their software clock must be set from an external time source via the Network Time Protocol (NTP). To provide a trusted time source for the TOE, NTP servers must be connected to a trusted network in a secure location.

## Access Control

The Cisco IOS router must be configured to authenticate privileged (enable mode) and unprivileged access to the CLI using a username or password. A good password has a combination of alphabetic and numeric characters, as well as punctuation characters. This password must be at least eight characters in length. We recommend that you tell the password to someone who is in a position of trust.

## Remote Administration and Management

If you administer and manage the Cisco IOS router from a remote management system across an untrusted network, the following requirements apply:

- The management station must be connected to a trusted network.
- There must be another Cisco IOS router connected to the trusted and untrusted network.
- There must be an IPSec tunnel between the trusted network and the Cisco IOS router that is managed.

A topology such as Figure 1, which displays these requirements, applies to any in-band administrative protocol including Telnet, Simple Network Management Protocol (SNMP), and syslog.

## SNMP

If SNMP read-write access is permitted, the TOE operation can be modified via SNMP. Therefore, SNMP must be configured explicitly in read-only mode if it is enabled on the TOE to support monitoring of the Cisco IOS router.

## Logging and Messages

Monitoring activity in the log files is an important aspect of your network security and should be conducted regularly. Monitoring the log files allows you take appropriate and timely action when you detect breaches of security or events that are likely to lead to a potential security breach.

To view log file messages, use the **show logging** EXEC command. For configuration details, refer to the section “Message Logging” in Table 6.

## Access Lists

The **access-list** command operates on a first match basis. Thus, the last rule added to the access list is the last rule checked. The administrator should make a note of the last rule during initial configuration because it may impact the remainder of the rule parsing.

To enable logging of access-list matches, use the **log** keyword with access-list definitions.

## Monitoring and Maintenance

There are several ways (from logs to messages) in which you can monitor the operation of your Cisco IOS routers. However, ensure you know how you will monitor the router for performance and possible security issues. Also, plan your backups; if there should be hardware or software problems, you may need to restore the router configuration.

# Installation Notes

Table 4 lists the documentation that should be used when installing a Cisco IOS IPSec evaluated router.

***Table 4 Installation Documentation for Cisco IOS IPSec Hardware Platforms***

| Hardware Family | Regulatory Compliance and Safety Information Documentation |
|---|---|
| Cisco 1700 series | *Cisco 1720 Series Router Hardware Installation Guide*<br>*Cisco 1750 Series Router Hardware Installation Guide*<br>*Installing the Data Encryption AIM in Cisco 1700 Series Routers*[1] |
| Cisco 2600 series | *Cisco 2600 Series Hardware Installation Guide*<br>*Installing the Data Encryption AIM in Cisco 2600 Series and Cisco 3600 Series Routers*[1] |

*Table 4 Installation Documentation for Cisco IOS IPSec Hardware Platforms (continued)*

| Hardware Family | Regulatory Compliance and Safety Information Documentation |
|---|---|
| Cisco 3600 series | *Cisco 3600 Series Hardware Installation Guide*<br>*Installing the Data Encryption AIM in Cisco 2600 Series and Cisco 3600 Series Routers*[1] |
| Cisco 7100 series | *Cisco 7100 Series VPN Router Installation and Configuration Guide*<br>*Integrated Service Adapter and Integrated Service Module Installation and Configuration*[1]<br>*VPN Acceleration Module Installation and Configuration*[1] |
| Cisco 7200 series | *Cisco 7204 Installation and Configuration Guide*<br>*Cisco 7206 Installation and Configuration Guide*<br>*Cisco 7200 VXR Installation and Configuration Guide*<br>*Integrated Service Adapter and Integrated Service Module Installation and Configuration*[1]<br>*VPN Acceleration Module Installation and Configuration*[1] |

[1] Hardware encryption acceleration modules are optional.

# Verification of Image and Hardware IPSec Module

To verify that the Cisco IOS software and hardware IPSec VPN module (if used) has not been tampered with during delivery, perform the following steps.

**Note** If a hardware IPSec VPN module is not being used, only steps 6 and 7 are necessary.

**Note** Hardware IPSec VPN modules are delivered either as separate discrete items or preinstalled in a Cisco router platform.

**Step 1** Inspect the physical packaging in which the equipment was delivered before unpacking the hardware IPSec VPN module.

- Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If the external packaging is not printed with Cisco branding, contact the equipment supplier (Cisco Systems or an authorized Cisco distributor or partner).

**Step 2** Verify that the packaging has not been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the equipment supplier.

**Step 3** Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar-coded label that is applied to the external cardboard box. (This label will include the Cisco product number, serial number, and other information regarding the contents of the box.) If this label is missing, contact the equipment supplier.

**Step 4** Note the serial number of the hardware IPSec VPN module on the shipping documentation. If the hardware IPSec VPN module has been preinstalled, the white label on the outer box will show the serial number of the router platform inside; thus, the serial number of the hardware IPSec VPN module will appear on the shipping documents also attached to the outer box. Otherwise, if the VPN has not been preinstalled, the serial number of the hardware IPSec VPN module will be displayed on the white label.

Ensure that the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If the serial numbers do not match, contact the equipment supplier.

**Step 5** Verify that the box has been shipped from the expected equipment supplier by performing the following tasks:

- Contact the supplier to verify that the box was shipped with the courier company that delivered the box and that the consignment note number for the shipment matches the number used for the delivery.
- Verify that the serial numbers of the items shipped match the serial numbers of the items delivered. For equipment shipped directly from Cisco, you can verify the serial numbers online through Cisco's Networking Products Marketplace, Order Status Tool. For other suppliers, verify that the serial numbers match by using a mechanism that was not involved in the actual equipment delivery; for example, use the phone, fax, or another online tracking service.

**Step 6** Inspect the module after the hardware IPSec VPN module has been unpacked. Verify that the serial number displayed on the module matches the serial number on the shipping documentation and the invoice. If the serial numbers do not match, contact the equipment supplier.

**Step 7** Download a Common Criteria evaluated software image file from Cisco Connection Online (CCO) for your specific hardware platform onto a trusted computer system (as specified in Table 1). For all images, ensure that you have sufficient system and Flash memory to support the image on your router hardware by checking the release notes appropriate for the Cisco IOS release and by selecting the IPSec 56 or IPSec 3DES feature set.

Software images for Release 12.2(6) are available from CCO at the following URL:
http://cco.cisco.com/kobayashi/library/12.2/index.shtml
Software images for Release 12.1(10)E available from CCO at the following URL:
http://cco.cisco.com/kobayashi/library/12.1/index.shtml

After you have downloaded the file, verify that the file has not been tampered with by using a Message Digest 5 (MD5) utility to compute an MD5 hash for the file; compare this MD5 hash with the MD5 hash for the image, which is listed in Table 9. If the MD5 hashes do not match, contact Cisco Technical Support.

**Step 8** Install the downloaded and verified software image onto your Cisco IOS router. For information on completing this task, refer to the chapter "Loading and Maintaining System Images" in the part "File Management" of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

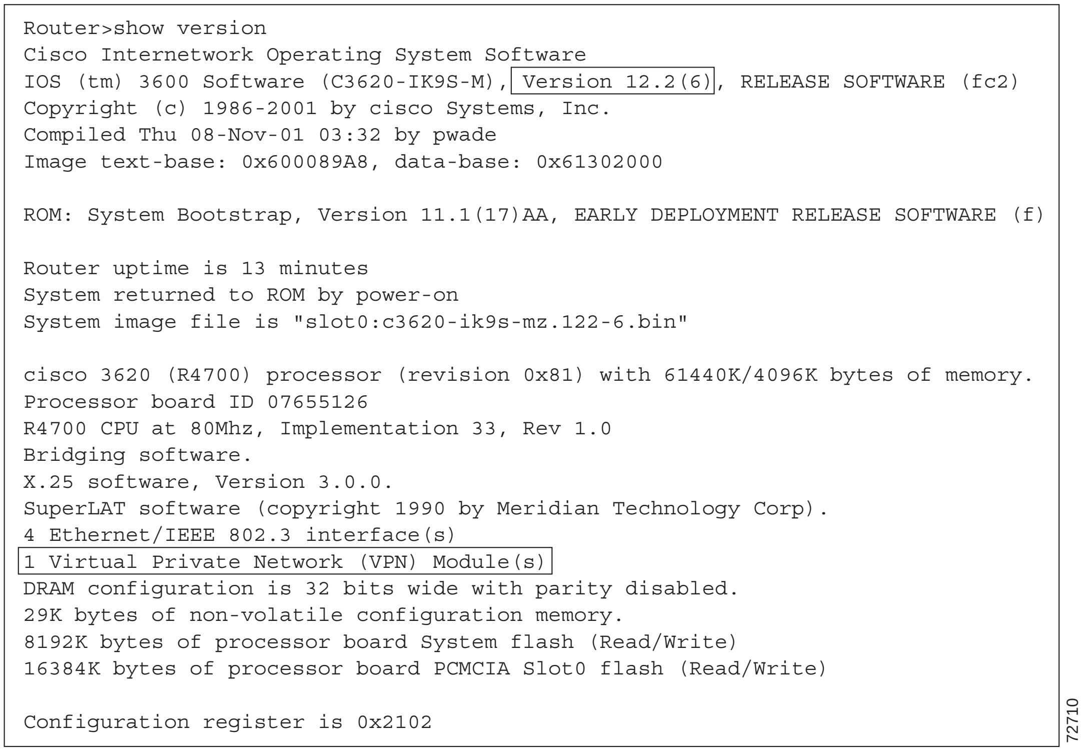
**Step 9** Start your router as described in the appropriate installation documentation that is outlined in Table 4. Confirm that your router loads the image correctly, completes internal self-checks, and displays the cryptographic export warning on the console. At the prompt, type the **show version** command. (See Figure 2.) Verify that the version matches one of the valid versions listed in Table 1. If the versions do not match or if the image fails to load, contact Cisco Technical Support.

**Step 10** If the hardware IPSec VPN module has not been preinstalled, refer to one of the installation guides in Table 4.

**Step 11** After the IPSec VPN module is installed, restart the router. At the prompt, enter the **show version** command. (See Figure 2.) To verify that a VPN module is installed, read the output display. If the output display does not report that the hardware IPSec VPN module is present, contact Cisco Technical Support.

**Step 12** Enter the **show diag** command. Examine the output to ensure that the serial number reported by the hardware IPSec VPN module is the same as the serial number on the shipping documentation, invoice, and the hardware IPSec VPN module itself. Also, verify that the hardware version and revision of the module are listed in Table 8.

***Figure 2 Sample show version Output That Shows the Cisco IOS Version and Presence of the Hardware IPSec VPN Module***



```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-IK9S-M), Version 12.2(6), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 08-Nov-01 03:32 by pwade
Image text-base: 0x600089A8, data-base: 0x61302000

ROM: System Bootstrap, Version 11.1(17)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (f)

Router uptime is 13 minutes
System returned to ROM by power-on
System image file is "slot0:c3620-ik9s-mz.122-6.bin"

cisco 3620 (R4700) processor (revision 0x81) with 61440K/4096K bytes of memory.
Processor board ID 07655126
R4700 CPU at 80Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
4 Ethernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Configuration register is 0x2102
```

# Configuration Notes

The Common Criteria TOE for Cisco IOS IPSec defines the following two groups of features:

- Security Enforcing
- Security Supporting

**Note** Upon delivery, a Cisco IOS router is not configured to support any of these security enforcing or supporting functions. To ensure that your router is operating in accordance with Common Criteria evaluated Cisco IOS IPSec, these functions must be explicitly configured as described in this document and in the appropriate product documentation.

## Security Enforcing

Security enforcing consists of the following functions:

- IPSec IKE using preshared keys, RSA keys, or digital certificates

**Note** Cisco 1700 series and Cisco 7200 series with an SM-VAM or SA-VAM do not support IKE with RSA keys.

- IPSec ESP using tunnel mode with DES or 3DES
- Optional hardware acceleration of IPSec (as specified in Table 1)
- Cryptographic key generation and management

For information on configuring these security enforcing functions, refer to the chapters in the part "IP Security and Encryption" of the *Cisco IOS Security Configuration Guide*. (If you are using the *Cisco IOS Security Configuration Guide*, Release 12.1, use all chapters within the part "IP Security and Encryption" except the chapter "Configuring Cisco Encryption Technology.")

To ensure that your Cisco IOS router configuration is consistent with Common Criteria evaluated Cisco IOS IPSec, you must consider the IPSec options listed in Table 5.

*Table 5 Evaluated Security Enforcing (IPSec) Options for Cisco IOS Routers*

| Configuration Command | Evaluated Options | Options Not Evaluated |
|---|---|---|
| **crypto map (global IPSec)** | ipsec-isakmp | ipsec-manual |
| **crypto ipsec transform-set** | esp-des | ah-md5-hmac |
| | esp-3des | ah-sha-md5 |
| | esp-md5-hmac | esp-null |
| | esp-sha-hmac | comp-lzs |
| **mode (IPSec)** | tunnel | transport |

## Security Supporting

Security supporting consists of the following functions:

- Inbound access lists
- Message logging
- User authentication for access to the CLI using locally configured passwords.

**Note** Although Cisco IOS supports AAA user authentication, it is not supported within Common Criteria evaluated Cisco IOS IPSec.

- Time management

Table 6 lists the documents that you should use to configure security supporting functions.

*Table 6 Documentation for Evaluated Security Supporting Functions*

| Feature | Cisco IOS Documentation |
|---|---|
| Inbound access lists | The chapter “Access Control Lists: Overview and Guidelines” in the part “Traffic Filtering and Firewalls” of the *Cisco IOS Security Configuration Guide*<br>The chapter “Configuring IP Services” in the section “IP Addressing and Services” of the *Cisco IOS IP Routing Configuring Guide* |
| Message logging | The chapter “Troubleshooting and Fault Management” in the section “System Management” of the *Cisco IOS Configuration Fundamentals Configuration Guide* |
| User authentication | The chapter “Configuring Passwords and Privileges” in the part “Other Security Features” of the *Cisco IOS Security Configuration Guide* |
| Time management | The chapter “Performing Basic System Management” in the part “System Management” of the *Cisco IOS Configuration Fundamentals Configuration Guide* |

### Saving Configurations

When making changes to the configuration of the router, use the **write memory** command frequently. If the router reboots and resumes operation when uncommitted changes have been made, these changes will be lost and the router will revert to the last configuration saved.

### Enabling Time Stamps

By default, all audit records are not stamped with the time and date, which are generated from the system clock when an event occurs.

The Common Criteria evaluated Cisco IOS IPSec requires that the time-stamp feature be enabled on your Cisco IOS router. To enable the time stamp of audit events, use the **service timestamps log datetime** command.

To ensure that the **timestamps** option is meaningful, the system clock in your router must be set correctly. (See the following section, “Setting the System Clock,” for more information.)

### Setting the System Clock

To provide accurate time stamps for logging and to ensure that your router can process validity dates for digital certificates, the system clock must be set. Some models of Cisco IOS routers have real-time clocks that maintain real time when the router is powered down; these real-time clocks are used to initialize the system clock at startup. Other models of Cisco IOS routers do not have a real-time clock and must obtain the correct date and time from a reliable time source using the NTP. One example of a reliable time source is a Cisco IOS router with a real-time clock operating as an NTP Server. Table 7 lists router clock functions for use with Cisco IOS IPSec.

*Table 7 Cisco IOS Router Clock Functions*

| Hardware Family | Real-time Clock | System Clock | Documentation |
|---|---|---|---|
| Cisco 1700 series<br>Cisco 2600 series<br>Cisco 3600 series | No | NTP client | The chapter “Performing Basic System Management” in the part “System Management” of the *Cisco IOS Configuration Fundamentals Configuration Guide* |
| Cisco 7100 series<br>Cisco 7200 series | Yes | Internal; can be NTP server | The chapter “Performing Basic System Management” in the part “System Management” of the *Cisco IOS Configuration Fundamentals Configuration Guide* |

# Hardware Versions of Hardware IPSec VPN Modules

Table 8 lists the hardware versions of IPSec VPN modules.

*Table 8 IPSec VPN Modules Hardware Versions*

| Product Name | Cisco Part Number and Revisions |
|---|---|
| SM-VAM | 73-5953-04 A0 |
| SM-VAM | 73-5953-05 A0 |
| SA-ISA | 73-4201-06 A0 |
| SM-ISM | 73-4201-06 B0 |
| | 73-4201-07 A0 |
| AIM-VPN/HP | 800-05255-01 A0 |
| | 800-05255-01 B0 |
| | 800-05255-02 A0 |
| | 800-05255-02 B0 |
| | 800-05255-03 A0 |
| | 800-05255-03 B0 |
| NM-VPN/MP | 800-05213-01 A0 |
| | 800-05213-01 B0 |
| | 800-05213-02 A0 |
| | 800-05213-02 B0 |
| | 800-05213-03 A0 |
| | 800-05213-03 B0 |

*Table 8 IPSec VPN Modules Hardware Versions (continued)*

| Product Name | Cisco Part Number and Revisions |
|---|---|
| AIM-VPN/BP | 800-05191-01 A0<br>800-05191-01 B0<br>800-05191-02 A0<br>800-05191-02 B0<br>800-05191-03 A0<br>800-05191-03 B0<br>800-05191-03 C0 |
| MOD1700-VPN | 73-4586-01 A0<br>73-4586-01 B0<br>73-4586-01 C0<br>73-4586-02 A0 |

# MD5 Hash Values for Cisco IOS Software Images

Table 9 lists the MD5 hash values for Cisco IOS software images.

*Table 9 Cisco IOS Software Images and MD5 Hash Values*

| Cisco IOS Image Name | Cisco IOS Feature Set | MD5 Hash of Cisco IOS Image |
|---|---|---|
| **Cisco 7200 with Release 12.2(6)** | | |
| c7200-a3jk8s-mz.122-6.bin | ENTERPRISE/SNASW IPSEC 56 | 2bba35bb3fb3ad57a3ae428dd89b68ab |
| c7200-dk8o3s-mz.122-6.bin | DESKTOP/IBM/FW/IDS IPSEC 56 | 3f6a6c346157db5bbe9802ba77d0e806 |
| c7200-dk8s-mz.122-6.bin | DESKTOP/IBM IPSEC 56 | 1f48c42614dc4e7389c3a36d491aebbc |
| c7200-ik8o3s-mz.122-6.bin | IP/FW/IDS IPSEC 56 | 33ed2cffb43269b129fddb5822b3dcb2 |
| c7200-ik8s-mz.122-6.bin | IP IPSEC 56 | 768c6fd72c1db12530e5f296a2c76f87 |
| c7200-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS IPSEC 56 | e4b5edcef0a1a37a64e7f71ad3ba11bc |
| c7200-jk8s-mz.122-6.bin | ENTERPRISE IPSEC 56 | 0c2459edd5c8cad4ec4c49506c7a1ef4 |
| c7200-a3jk9s-mz.122-6.bin | ENTERPRISE/SNASW IPSEC 3DES | 23d373ec8d412318d2cc7fb151708b06 |
| c7200-dk9o3s-mz.122-6.bin | DESKTOP/IBM/FW/IDS IPSEC 3DES | bf41ec3b330a129ad1f7c5c786171f66 |
| c7200-ik9o3s-mz.122-6.bin | IP/FW/IDS IPSEC 3DES | cd30fbe49b47092044b23605012a1b63 |
| c7200-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | 2da99cd5f38c1690ee9471a98abfd439 |
| c7200-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS IPSEC 3DES | 55113e61674e9de6127902fca801042f |
| c7200-jk9s-mz.122-6.bin | ENTERPRISE IPSEC 3DES | 3ffabb0a54e17d9477b2555540fe4c70 |
| **Cisco 7100 with Release 12.2(6)** | | |
| c7100-ik8o3s-mz.122-6.bin | IP/FW/IDS IPSEC 56 | ca9bee44204316eead04a3c8a4336267 |

*Table 9 Cisco IOS Software Images and MD5 Hash Values (continued)*

| | | |
|---|---|---|
| c7100-ik8s-mz.122-6.bin | IP IPSEC 56 | a3ced0fe829ad7c40a6777afaa005b0e |
| c7100-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS IPSEC 56 | eef9dc5fea1161c20463d43ab2a9a690 |
| c7100-jk8s-mz.122-6.bin | ENTERPRISE IPSEC 56 | a3602b17af5326c481f025304c9f484a |
| c7100-ik9o3s-mz.122-6.bin | IP/FW/IDS IPSEC 3DES | f3a8931ee123b3e9c00be8f0eb089135 |
| c7100-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | 89af8e880183966df771342380e9e187 |
| c7100-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | 13892de3e4b2fa41281cb1d43bf6c466 |
| c7100-jk9s-mz.122-6.bin | ENTERPRISE IPSEC 3DES | 18cc0684514e139632f5acaede74ef85 |
| **Cisco 3660 with Release 12.2(6)** | | |
| c3660-a3jk8s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 56 | 577561c774dcda1d071b6d0532f81525 |
| c3660-ik8o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 56 | 4603a8418270ebc10f566c96cc14be0f |
| c3660-ik8s-mz.122-6.bin | IP PLUS IPSEC 56 | f3dd2581c7e0dd53aec57dfd011c7333 |
| c3660-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 56 | 48385b255a67d79b3353fb1586b1a035 |
| c3660-jk8s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 56 | 36e2be7a4a4d1c93287e92adf89d1ff5 |
| c3660-a3jk9s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 3DES | e3496987d62172ac1c857c36b963274e |
| c3660-ik9o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 3DES | 55f4b6acfdd66b8af01b429b86e8cc9c |
| c3660-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | b280c20a3497497114901f9e2adddb1a |
| c3660-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | f24bb356009043608c6b296d8833eaed |
| c3660-jk9s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 3DES | 0757b1cb6542ef313e5185a933199769 |
| c3660-telcoentk9-mz.122-6.bin | TELCO PLUS FEATURE SET IPSEC 3DES | c9d2e81d481694d1fa8f880ea6ae5483 |
| **Cisco 3640 with Release 12.2(6)** | | |
| c3640-a3jk8s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 56 | 64628ec89ef2fedc42e7f0219fc9a452 |
| c3640-ik8o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 56 | 3b10309c8579b01eac782a81a578ee8e |
| c3640-ik8s-mz.122-6.bin | IP PLUS IPSEC 56 | 2a46dc9d669b58066f0765be2b22404d |
| c3640-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 56 | 8c25d0115b66bef3212a8f3a7c29da06 |
| c3640-jk8s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 56 | 6bef9253e93eb7d83398513c34f9352d |
| c3640-a3jk9s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 3DES | c79a35c30a3765771b66cbdd4296539c |
| c3640-ik9o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 3DES | ddb8fee165877102d0f8f99855ee5ef4 |
| c3640-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | ce948b710f9ab9422574a9ef5ea482cd |
| c3640-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | dc4c0a9c29726fb54bcbdd60fcfd7770 |
| c3640-jk9s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 3DES | 3a4541c32e1f822407da77e07cdaeb1b |

*Table 9 Cisco IOS Software Images and MD5 Hash Values (continued)*

| **Cisco 3620 with Release 12.2(6)** | | |
|---|---|---|
| c3620-a3jk8s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 56 | b8bc2a854ce9c593576d0c22df911ffb |
| c3620-ik8o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 56 | 5d581350115e34ecd5a95849776edcc3 |
| c3620-ik8s-mz.122-6.bin | IP PLUS IPSEC 56 | 3a41053365bb5997bff0f2b723659e12 |
| c3620-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 56 | 5126fac09c7c6285ca690d48c62a541f |
| c3620-jk8s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 56 | 77bb989d83777634d0d3bcd7390acf56 |
| c3620-a3jk9s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 3DES | c3126eb3d24bcf2f39f4740c5cdf5501 |
| c3620-ik9o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 3DES | 02f7a7ee7f350a93f25046abd62e3ac5 |
| c3620-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | d7b34c3fb5c9789dd573e42c92d19470 |
| c3620-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | 3c7a7b74d9de5eda9ce4e586947626d8 |
| c3620-jk9s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 3DES | 2ce8f930608141e0837e8dd13befc846 |
| **Cisco 2610, 2611, 2612, 2613, 2620, 2621 with Release 12.2(6)** | | |
| c2600-a3jk8s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 56 | 86538a8ce471bbfaf80810c2b6a4d0cf |
| c2600-ik8o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 56 | 4738d6597f8933548e4dcd1e9b8e610f |
| c2600-ik8s-mz.122-6.bin | IP PLUS IPSEC 56 | 6641d9b29a71e9c2d3d44e113a32b6b0 |
| c2600-jk8o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 56 | 9a1f1cafbfb634ad7dd24d7f67a320ec |
| c2600-jk8s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 56 | 34cc47b34ca5c64e24199e4261826cd8 |
| c2600-a3jk9s-mz.122-6.bin | ENTERPRISE/SNASW PLUS IPSEC 3DES | c3fdc6e04b4a004cabe745221a3110d1 |
| c2600-ik9o3s-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 3DES | 4c3d7dc8812ae4fff08a2dbd3d536589 |
| c2600-ik9s-mz.122-6.bin | IP PLUS IPSEC 3DES | d15df41a51d57bba2ddfff3e38f38c95 |
| c2600-jk9o3s-mz.122-6.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | a90eb23c2370a810bfd1702788c9ccce |
| c2600-jk9s-mz.122-6.bin | ENTERPRISE PLUS IPSEC 3DES | 08c63c3c9ba4942e5ce097bd38805ff3 |
| **Cisco 1750 with Release 12.2(6)** | | |
| c1700-bk8no3r2sv3y-mz.122-6.bin | IP/IPX/AT/IBM/VOICE/FW/IDS PLUS IPSEC 56 | fe365f6b9233dbc861ab6f7dafe95b78 |
| c1700-k8o3sv3y-mz.122-6.bin | IP/VOICE/FW/IDS PLUS IPSEC 56 | 366c0728a7d33b06f688c72b4a9df8c1 |
| c1700-k8sv3y-mz.122-6.bin | IP/VOICE PLUS IPSEC 56 | cf5fb5c321ca166737bf9b879510f5d0 |
| c1700-bk9no3r2sv3y-mz.122-6.bin | IP/IPX/AT/IBM/VO/FW/IDS PLUS IPSEC 3DES | 39131f81690552319552d5dc926a7a30 |
| c1700-k9o3sv3y-mz.122-6.bin | IP/VOICE/FW/IDS PLUS IPSEC 3DES | 7a39d0528439b787aaa6f200af8fabb9 |
| c1700-k9sv3y-mz.122-6.bin | IP/VOICE PLUS IPSEC 3DES | c398b885becaa574bbc21775a4b9cd1c |

*Table 9 Cisco IOS Software Images and MD5 Hash Values (continued)*

| | | |
|---|---|---|
| **Cisco 1720 with Release 12.2(6)** | | |
| c1700-bk8no3r2sy-mz.122-6.bin | IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 56 | 3a68e7c3edf00e4947dec02de2215742 |
| c1700-k8o3sy-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 56 | 075a7dc676c0f7fdaae98400d78fca76 |
| c1700-k8sy-mz.122-6.bin | IP PLUS IPSEC 56 | 2a7bba62a26c790ad0c1a667e28b5010 |
| c1700-bk9no3r2sy-mz.122-6.bin | IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES | dbb2e4dac4dbba36ce4ec4f7da4c12d0 |
| c1700-k9o3sy-mz.122-6.bin | IP/FW/IDS PLUS IPSEC 3DES | ce2eab199ca8359c214ecfb48e34e988 |
| c1700-k9sy-mz.122-6.bin | IP PLUS IPSEC 3DES | eaa02f8cc86da69c20a73753df99aa3d |
| **Cisco 7200 with Release 12.1(10)E** | | |
| c7200-do3s56i-mz.121-10.E.bin | DESKTOP/IBM/FW/IDS IPSEC 56 | b26914e12a462d2bddc24951a5878cde |
| c7200-ds56i-mz.121-10.E.bin | DESKTOP/IBM IPSEC 56 | b16e652f01b5b99337cedfa63392a840 |
| c7200-io3s56i-mz.121-10.E.bin | IP/FW/IDS IPSEC 56 | 708dece58caf4f1aaf63a4ff0dd53a97 |
| c7200-is56i-mz.121-10.E.bin | IP IPSEC 56 | f28797dd82ca3c51ba084a8df5b93fc9 |
| c7200-jo3s56i-mz.121-10.E.bin | ENTERPRISE/FW/IDS IPSEC 56 | c3dad78a560ad6c4f402e641939be015 |
| c7200-js56i-mz.121-10.E.bin | ENTERPRISE IPSEC 56 | b2068f05d074f60650be967781e74701 |
| c7200-dk2o3s-mz.121-10.E.bin | DESKTOP/IBM/FW/IDS IPSEC 3DES | 6044f68393adeb3900f0249beecc4c43 |
| c7200-ik2o3s-mz.121-10.E.bin | IP/FW/IDS IPSEC 3DES | 54e767b0ed4e0f953c330ca36fbe1396 |
| c7200-ik2s-mz.121-10.E.bin | IP PLUS IPSEC 3DES | 022e757fcccc0efec403e7ab0b48759b |
| c7200-jk2o3s-mz.121-10.E.bin | ENTERPRISE/FW/IDS IPSEC 3DES | cc042f8972b75c841cd4e8740cbae9e4 |
| c7200-jk2s-mz.121-10.E.bin | ENTERPRISE IPSEC 3DES | 3b5b54158a719cdcd1573fa75fa88acd |
| **Cisco 7100 with Release 12.1(10)E** | | |
| c7100-io3s56i-mz.121-10.E.bin | IP/FW/IDS IPSEC 56 | 6a3fe1d410ead1f5ef01c8a0dc7338af |
| c7100-is56i-mz.121-10.E.bin | IP IPSEC 56 | 3f14e2c1a0dcab28531516f31ddbc4c8 |
| c7100-jo3s56i-mz.121-10.E.bin | ENTERPRISE/FW/IDS IPSEC 56 | e29bcda00e4deabc8f60667c42de5b35 |
| c7100-js56i-mz.121-10.E.bin | ENTERPRISE IPSEC 56 | 3b9e4ba61194994c61bc83a8334ddf44 |
| c7100-ik2o3s-mz.121-10.E.bin | IP/FW/IDS IPSEC 3DES | f73fbdd8cb69a7bb5822ecfb1f40ad01 |
| c7100-ik2s-mz.121-10.E.bin | IP PLUS IPSEC 3DES | fbec1edbde89408eca5b1dd680c9c39c |
| c7100-jk2o3s-mz.121-10.E.bin | ENTERPRISE/FW/IDS PLUS IPSEC 3DES | ff1ca727b58614369306fa600eacfc41 |
| c7100-jk2s-mz.121-10.E.bin | ENTERPRISE IPSEC 3DES | f052d9acbeb51ddb4f486f90d228e6ba |

For verification of MD5 hash values, contact Cisco Technical Support.

# Related Documentation

Use this document in conjunction with the appropriate Cisco IOS software documentation, which can be found at the following location:

Documentation for Cisco IOS Release 12.1:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm

Documentation for Cisco IOS Release 12.2:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm

# Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

## World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

http://www.cisco.com

Translated documentation is available at the following website:

http://www.cisco.com/public/countries_languages.html

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

# Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

## Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.