Installation and Configuration for Common Criteria EAL2 Evaluated Cisco IOS IPSec

January 2007

This document describes how to install and configure Cisco IOS routers in accordance with the Common Criteria Evaluation Assurance Level 2 (EAL2) 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:

Americas 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 12.2 and 12.4 documentation sets, which should be read prior to configuring a Cisco IOS router in accordance with the Common Criteria Evaluation Assurance Level 2 (EAL2) evaluated Cisco IOS IPSec.

Cisco product documentation includes

- Configuration Guides, which provide a descriptive overview of functions, the commands needed to enable them, and the sequence of operations that should be followed to implement them. The configuration guide should be consulted first when enabling features and functions.
- Command References, which provide a complete and detailed summary of all configuration commands and options, their effects, and examples and guidelines for their use. The command references should be consulted to confirm detailed syntax and functionality options.
- Error Message summaries, which describe all error messages issued by the product.

When this guide refers to a Cisco document, the title is listed and the filename (as available on www.cisco.com) is provided in brackets. The following Cisco IOS Release 12.2 and 12.4 documentation is referenced by this document:

- Regulatory Compliance and Safety Information specific to each router platform (Table 2)
- Hardware Installation Guides for each router platform (Table 4)
- *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2 (fcfbook.pdf)
- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4, File Management, Loading and Maintaining System Images (cfh900.pdf)
- *Cisco IOS Security Configuration Guide*, Release 12.4, Part 4: Implementing IPSec and IKE, “Configuring Internet Key Exchange for IPSec VPNs” (sec_ike.pdf)
- *Cisco IOS Security Configuration Guide*, Release 12.4, Part 4: Implementing IPSec and IKE, “Configuring Security for VPNs with IPSec” (sec_ipse.pdf)
- *Cisco IOS Security Configuration Guide*, Release 12.4, Part 3: Traffic Filtering, Firewalls, and Virus Detection, “Access Control Lists: Overview and Guidelines” (schacls.pdf)
- *Cisco IOS IP Application Services Command Reference*, Release 12.4 (apl_bokh.pdf)
- *Cisco IOS IP Application Services Command Reference*, Release 12.2SR (iap_a1sr.pdf)
- *Cisco IOS Network Management Configuration Guide*, Release 12.4, Part 3: System and Network Management, “Troubleshooting and Fault Management” (fcf013.pdf)
- *Cisco IOS Security Configuration Guide*, Release 12.4, Part 1: Authentication, Authorization, and Accounting (AAA), “Configuring Authentication, Configuring Authentication” (schathen.pdf)
- *Cisco IOS Network Management Configuration Guide*, Release 12.4, Part 3: System and Network Management, “Performing Basic System Management” (fcf012.pdf)

Cisco IOS documentation is available on CD-ROM, in printed-paper form, and online (in both HTML and PDF formats). This document may be used in conjunction with the August 2006 Cisco IOS IPSec Evaluation Documentation DVD-ROM available upon request from Cisco Systems by sending an email to CC-Doc-Request@cisco.com.

The Cisco IOS documents listed above can also be found online at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/index.htm

Audience

This document is written for administrators configuring a Cisco IOS router in accordance with the Common Criteria evaluated Cisco IOS IPSec. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you have been trained for use with IPSec technology and its applications; for example, site-to-site Virtual Private Networks (VPNs). There are no components of the Cisco IP System that are accessible to non-administrative users (end-users), and hence there is no user-level documentation.

Supported Hardware and Software Versions

The hardware and software combinations that are complaint with Common Criteria evaluated Cisco IOS IPSec are outlined in Table 1. To display the hardware version of an IPSec/VPN Hardware module, use the **show diag** command.

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

Hardware Family	Supported Models	IPSec Hardware Acceleration Module[1]	Cisco IOS Release
Cisco 800 series	871, 876, 877, 878, 851, 851W, 857, 857W	Built In	Cisco IOS 12.4(6)T3
Cisco 1800 series	1841	optionally with AIM-VPN/BPII-PLUS	Cisco IOS 12.4(7)
	1801, 1802, 1803, 1811, 1812	Built In	Cisco IOS 12.4(6)T3
Cisco 2800 series	2801,2811, 2821, 2851	optionally with AIM-VPN/EPII-PLUS	Cisco IOS 12.4(7)
Cisco 3800 series	3825	optionally with AIM-VPN/EPII-PLUS	Cisco IOS 12.4(7)
	3845	optionally with AIM-VPN/HPII-PLUS	Cisco IOS 12.4(7)
Cisco 7200 series	7204, 7206	SA-VAM2+	Cisco IOS 12.4(7)
Cisco 7300 series	7301	SA-VAM2+	Cisco IOS 12.4(7)
Cisco 7600 Catalyst 6500	Any 6500 or 7600 with Supervisor Engine 720, 720-3B, or 720-3BXL	SPA-IPSEC-2G	Cisco IOS 12.2(33)SRA

1. Support for RSA public/private key pairs for IKE authentication requires the use of an IPSec hardware acceleration module. Models listed as using “Built In” modules do not support RSA public/private key pairs for IKE authentication.

Security Information

This section contains the following sections:

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 800 series routers	*Regulatory Compliance and Safety Information for the Cisco 800 Series and SOHO Series Routers* (800srcsi.pdf)
Cisco 1800 Series Integrated Services Routers	*Regulatory Compliance and Safety Information for Cisco 1800 Series Integrated Services Routers* (Fixed) (cuisrcsi.pdf) *Regulatory Compliance and Safety Information for Cisco 1840 Routers* (1800rcsi.pdf)
Cisco 2800 Series and Cisco 3800 Integrated Services Routers	*Cisco 2800 Series and Cisco 3800 Series Integrated Services Routers Regulatory Compliance and Safety Information* (2838rsci.pdf)
Cisco 7200 Series Routers	*Cisco 7200 Regulatory Compliance and Safety Information* (3419pnc6.pdf)
Cisco 7300 Series Routers	*Regulatory Compliance and Safety Information for the Cisco 7301 Internet Router* (16178r.pdf)
Cisco 7600 Series Routers	*Regulatory Compliance and Safety Information for the Cisco 7600 Series Routers* (78_13690.pdf)
Cisco Catalyst 6500 Series Switches	*Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches* (78_12928.pdf)

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

- Which networks 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/destination IP address and/or port number
- The Cisco IOS routers 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 to be considered untrusted and trusted. An untrusted interface is one that is connected to an untrusted network over which the administrator wishes to send and receive trusted traffic protected by IPSec encryption.

Figure 1 Organizational Security Policy Example

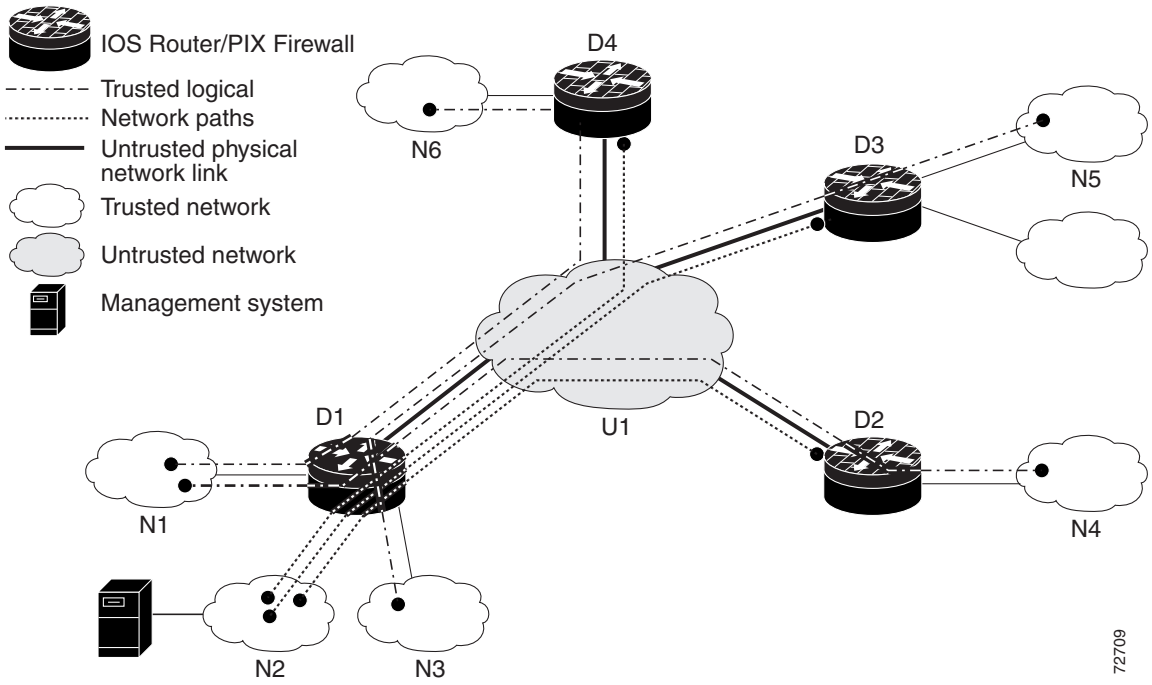

Figure 1 displays an organizational security policy with traffic flows that are identified solely by source and destination IP addresses. All Cisco IOS routers (D1, D2, D3, and D4) must be configured to implement a portion of the organizational security policy. For example, Router D1 has three trusted 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 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 IKE using preshared keys, RSA keys[1], or digital certificates

Note The AIM-VPN/BPII, AIM-VPN/EPII, AIM-VPN/HPII, and VAM2 do not support IKE with RSA keys for IKE authentication.

- IPSec encapsulating security payload (ESP) using tunnel or transport mode with Data Encryption Standard (DES) or 3DES
- 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 accounts
- 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 EAL2).

1. Support for RSA public/private key pairs for IKE authentication requires the use of an IPSec hardware acceleration module. Models listed as using “Built In” modules do not support RSA public/private key pairs for IKE authentication

Time Sources

Routers configured in accordance with the Cisco IOS IPSec evaluation must timestamp system log messages. For Cisco routers without internal real time hardware clocks (800 series) their software clock must be set from an external time source via the Network Time Protocol (NTP). NTP servers must be connected to a trusted network in a secure location to be able to provide a trusted time source for the TOE.

Access Control

The Cisco IOS Router must be configured to authenticate both unprivileged and privileged (enable mode) access to the CLI using a username and 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 long. 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, that displays these requirements, applies to any in-band administrative protocol including Telnet, Simple Network Management Protocol (SNMP), and syslog.

SNMP

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

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. Therefore, 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, the **log** keyword should be used 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	Installation Information
Cisco 800 Series Routers	*Cisco 850 Series and Cisco 870 Series Access Routers Cabling and Setup Quick Start Guid*e (857qseng.pdf)
Cisco 1800 Series Integrated Services Routers	*Cisco 1801, Cisco 1802, and Cisco 1803 Integrated Services Routers Cabling and Installation* (1801qsg.pdf) *Cisco 1811 and 1812 Integrated Services Router Cabling and Installation* (1811qsg.pdf) *Cisco 1800 Series Integrated Services Router (Modular) Quick Start Guide* (1800qsg.pdf)
Cisco 2800 Series Integrated Services Routers	*Cisco 2800 Series Integrated Services Routers Quick Start Guide* (2800_qsg.pdf) *Installing and Upgrading Internal Modules in Cisco 2800 Series Routers* (10_hw.pdf)
Cisco 3800 Series Integrated Services Routers	*Cisco 3800 Series Integrated Services Routers Quick Start Guide* (rb_qsg.pdf) *Installing and Upgrading Internal Components in Cisco 3800 Series Routers* (38comp.pdf)
Cisco 7200 Series Routers	*Cisco 7204 Installation and Configuration Guide* (ccmigration_09186a0080202513.pdf) *Cisco 7206 Installation and Configuration Guide (ccmigration_09186a0080201fb9.pdf)* *SA-VAM2+ Installation and Configuration Guide* (ccmigration_09186a00803e0217.pdf)
Cisco 7300 Series Routers	*Cisco 7301 Installation and Configuration Guide* (ccmigration_09186a00804a5822.pdf) *SA-VAM2+ Installation and Configuration Guide* (ccmigration_09186a00803e0217.pdf)

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

Hardware Family	Installation Information
Cisco 7600 Series Routers	*Installing the Cisco 7600 Series Router* (instal.pdf) *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide* (ccmigration_09186a008043f8e6.pdf)
Cisco Catalyst 6500 Series Switches	*Catalyst 6500 Series Switches Installation Guide* (ccmigration_09186a0080231ba4.pdf) *Catalyst 6500 Series Switch SIP, SSC, and SPA Hardware Installation Guide* (ccmigration_09186a00805f53dd.pdf)

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 indeed been shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner) 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 the Order Status Tool (requires a cisco.com login). The Order Status Tool can be accessed from http://cco.cisco.com/en/US/partner/ordering/index.shtml or directly via http://cco.cisco.com/cgi-bin/status. 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.com 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 appropriate feature set as listed in Table 10.

Software images are available from Cisco.com at the following URL:
http://cco.cisco.com/kobayashi/library/12.4/index.shtml
http://cco.cisco.com/kobayashi/library/12.2/index.shtml

Step 8 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 9 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 and Network Management Configuration Guide*.

Step 10 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 11 If the hardware IPSec VPN module has not been preinstalled, refer to one of the installation guides in Table 4.

Step 12 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 13 Enter the **show diag** command for the Cisco 800, 1800, 2800, 3800, 7200 and 7300 series routers; enter the **show idprom module** *module* (for example 3/0) (see Figure 3) for the Cisco 6500 and 7500 series routers. Examine the output to verify that the serial number reported by the hardware IPSec VPN module is the same as the serial number on the shipping documentation and invoice (see Step 4), and displayed on the hardware IPSec VPN module itself (see Step 5). At the same time, verify that the hardware version and revision of the module are listed in Table 9.

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) 7200 Software (C7200-IK9S-M), Version 12.3(6a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 27-Oct-03 15:10 by kellythw
Image text-base: 0x60008AF4, data-base: 0x61E02000

ROM: System Bootstrap, Version 12.0(19990210:195103) [12.0XE 105], DEVELOPMENT S
OFTWARE
BOOTLDR: 7200 Software (C7200-BOOT-M), Version 12.0(21)ST2, EARLY DEPLOYMENT REL
EASE SOFTWARE (fc1)

Router uptime is 0 minutes
System returned to ROM by reload at 15:06:31 AEST Mon Dec 1 2003
System restarted at 15:08:46 AEST Mon Dec 1 2003
System image file is "slot1:c7200-ik9s-mz.123-6a.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 7206VXR (NPE300) processor (revision B) with 122880K/40960K bytes of memory.
Processor board ID 15456690
R7000 CPU at 262MHz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.

PCI bus mb0_mb1 has 540 bandwidth points
PCI bus mb2 has 500 bandwidth points

4 Ethernet/IEEE 802.3 interface(s)
3 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
1 ATM network interface(s)
1 Integrated service adapter(s)
125K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
Router>
```

230578

Figure 3 Sample show idprom module 3/0 Output That Shows the IPSec VPN Module Serial Number

```
7604_Router#show idprom module 3/0
IDPROM for SPA module #3/0
 (FRU is 'IPSec Shared Port Adapter with 2 Gbps DES/3DES/AES')
 Product Identifier (PID) : SPA-IPSEC-2G
 Version Identifier (VID) : V01
 PCB Serial Number        : JAB100809MK
 Top Assy. Part Number    : 68-2163-02
 Top Assy. Revision       : B0
 Hardware Revision        : 1.0
 CLEI Code                : CNUCAC0AAA
```

230579

Configuration Notes

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

- Security Enforcing
  - IPSec IKE using pre-shared keys, RSA keys or digital certificates
  - IPSec ESP using tunnel or transport mode with 3DES or AES
  - Hardware acceleration of IPSec (see Table 1)
  - Cryptographic key generation and management
- Security Supporting
  - Inbound access-lists
  - Message logging
  - User authentication for access to the Command Line Interface using locally configured accounts
  - Time management

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 features should be configured as described in the following sections of the *Cisco IOS Security Configuration Guide*

- Configuring Internet Key Exchange for IPSec VPNs (sec_ike.pdf)
- Configuring Security for VPNs with IPSec (sec_ipse.pdf)

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-aes esp-aes 192 esp-aes 256 esp-3des esp-md5-hmac esp-sha-hmac	ah-md5-hmac ah-sha-md5 esp-null comp-lzs
mode (IPSec)	tunnel transport	—

Security Supporting

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" (schacls.pdf) in the part "Traffic Filtering and Firewalls" of the *Cisco IOS Security Configuration Guide* **Specific commands available as follows:** *Cisco IOS IP Application Services Command Reference*, Release 12.4 (apl_bokh.pdf) *Cisco IOS IP Application Services Command Reference*, Release 12.2SR (iap_a1sr.pdf)
Message logging	The chapter "Troubleshooting and Fault Management" (fcf013.pdf) in the section "System and Network Management" of the *Cisco IOS Network Management Configuration Guide*
User authentication	The chapter "Configuring Authentication" (schathen.pdf) in the part "Configuring Authentication, Authorization, and Accounting (AAA)" of the *Cisco IOS Security Configuration Guide*
Time management	The chapter "Performing Basic System Management" (fcf012.pdf) in the part "System and Network Management" of the *Cisco IOS Network Management 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 800 series	No	NTP client	The chapter "Performing Basic System Management" (fcf012.pdf) in the part "System and Network Management" of the *Cisco IOS Network Management Configuration Guide*
Cisco 1800 series Cisco 2800series Cisco 3800 series Cisco 7200s eries Cisco 7300 series Cisco 7600 series Cisco 6500 series	Yes	Internal; can be NTP server	

Hardware Versions of Hardware IPSec VPN Modules

Table 8 lists the hardware versions of IPSec VPN modules.

Table 8 IPSec VPN Acceleration Modules Hardware Versions

Product Name	Cisco Part Number and Revisions
SPA-IPSEC-2G	68-2163-02, B0
SA-VAM2+	68-2288-05, C0
AIM-VPN/HPII-PLUS	800-24800-01, D0
AIM-VPN/EPII-PLUS	800-24799-01, D0
AIM-VPN/BPII-PLUS	800-24660-01, D0

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	MD5 Hash of Cisco IOS Image
Cisco 800 Series with Cisco IOS Release 12.4(6)T3	
c850-advsecurityk9-mz.124-6.T3.bin ADVANCED SECURITY	c4bd5187701462084d2589e2b9de61fd
c870-adventerprisek9-mz.124-6.T3.bin ADVANCED ENTERPRISE SERVICES	f22ff2fdaa71d66f35a7a1f68051ed9a
c870-advipservicesk9-mz.124-6.T3.bin ADVANCED IP SERVICES	05033440d070b3244d296ed6a79a3cc8
c870-advsecurityk9-mz.124-6.T3.bin ADVANCED SECURITY	06bada2c07e72a95015bbdefed16f618
Cisco 1800 Series with Cisco IOS Release 12.4(6)T3	
c180x-adventerprisek9-mz.124-6.T3.bin ADVANCED ENTERPRISE SERVICES	628c4b1c1f1dc2ce26ee51250daf27b1
c180x-advipservicesk9-mz.124-6.T3.bin ADVANCED IP SERVICES	0929dc7c373797d6bce128e34a3d82b8
c180x-broadband-mz.124-6.T3.bin IP BROADBAND	a3d7d6def37897af8a038dbc8b29e043
Cisco 1841 with Cisco IOS Release 12.4(7)	
c1841-adventerprisek9-mz.124-7.bin BB-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	a2ec38937acca45bc6957341e5659cdd
c1841-advipservicesk9-mz.124-7.bin AISK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	df4f47da0e2ed00f904d86f3fc058689
c1841-advsecurityk9-mz.124-7.bin ASK9-ASK9 FEAT SET FACTORY UPG FOR BUNDLES	84c564ecd7293dccee50f7e256af29bb
c1841-broadband-mz.124-7.bin BB-BB FEAT SET FACTORY UPG FOR BUNDLES	a90b39db26dbfc3a364a0ebaf93c532d
c1841-entbasek9-mz.124-7.bin ENTERPRISE BASE	3cf196065436880bae6b28f37496cd4c
c1841-entservicesk9-mz.124-7.bin ENTERPRISE SERVICES	f8956ca2d6d2372b10a8c2c629c92ed6
c1841-ipbasek9-mz.124-7.bin IP BASE	0bfa2da5c9b439e2c0a7ad18ed6fa4f5
c1841-spservicesk9-mz.124-7.bin SPSK9-SPSK9 FEAT SET FACTORY UPG FOR BUNDLES	2d5351f0591a876ea997177f654a5f27

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

Cisco IOS Image Name	MD5 Hash of Cisco IOS Image
Cisco 2800 Series with Cisco IOS Release 12.4(7)	
c2800nm-adventerprisek9-mz.124-7.bin AISK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	6e248f5ffbee21e1ecab3cde0fa81157
c2800nm-adventerprisek9_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIPGW, TDMIP GW AES	4e5ebb8e2b7dc10c480d34843da2f7a7
c2800nm-advipservicesk9-mz.124-7.bin SPSK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	91aa2680afc3b49ffb8841cb439ef7e8
c2800nm-advsecurityk9-mz.124-7.bin ADVANCED SECURITY	5fb79445fc76f949c1b1aba4cf315d6d
c2800nm-entbasek9-mz.124-7.bin ENTERPRISE BASE	89ecf582fd7d45f6db302e9269ca13ab
c2800nm-entservicesk9-mz.124-7.bin SPSK9-ESK9 FEAT SET FACTORY UPG FOR BUNDLES	1aca5d095e8803548f4e9d7c9a51be22
c2800nm-ipbasek9-mz.124-7.bin IP BASE	3bcdb83256f1277c7cc6e6082efc8c82
c2800nm-ipvoice_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIP GW, TDMIP GW	e67418957f004d20ecd82182ceb2ce32
c2800nm-ipvoicek9-mz.124-7.bin IP VOICE	6f086c22f363b9be1ff773f2bf182ccc
c2800nm-spservicesk9-mz.124-7.bin SP SERVICES	7ae5f5d5eb91f5244573a02eeb00549d
c2801-adventerprisek9-mz.124-7.bin ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	71f68a04baffe940bf4ed2708d88874e
c2801-advipservicesk9-mz.124-7.bin SPSK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	8814e37d3ed66ffe270c17ed88ebe4d8
c2801-advsecurityk9-mz.124-7.bin ADVANCED SECURITY	e79dbc1bb7e8080cf9b17a35fa85bfb7
c2801-entbasek9-mz.124-7.bin ENTERPRISE BASE	aa9ae7d830800165798fe372b2f57a01
c2801-entservicesk9-mz.124-7.bin ENTERPRISE SERVICES	4acaa91bb64207734db611447201a7c3
c2801-ipbasek9-mz.124-7.bin IP BASE	4d39f05662beaf6f158dddb971714509
c2801-ipvoicek9-mz.124-7.bin IP VOICE	cc4f654444de4935cb726cc071c0fa67
c2801-spservicesk9-mz.124-7.bin SPSK9-SPSK9 FEAT SET FACTORY UPG FOR BUNDLES	179b2826ac790a47a5aa7214000d59d9

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

Cisco IOS Image Name	MD5 Hash of Cisco IOS Image
Cisco 3800 Series with Cisco IOS Release 12.4(7)	
c3825-adventerprisek9-mz.124-7.bin ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	528b2ced540287d97451329e0ca6793d
c3825-adventerprisek9_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIPGW, TDMIP GW AES	4f36b44544c8a0b863b1d9e52199c72c
c3825-advipservicesk9-mz.124-7.bin ASK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	d01968dc92a36972513235ec95170f8e
c3825-advsecurityk9-mz.124-7.bin ADVANCED SECURITY	70302c9c0d16feb78b657171170fa6aa
c3825-entbasek9-mz.124-7.bin ENTERPRISE BASE	054d3d85f9b917d37602fa5dda2be361
c3825-entservicesk9-mz.124-7.bin ENTERPRISE SERVICES	df417ba7859f8d82aa2c853f71651b17
c3825-ipbasek9-mz.124-7.bin IP BASE	e2bedd8643d3d5569c4d94bc4e3101df
c3825-ipvoice_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIP GW, TDMIP GW	d713cffe5829bd6da381933560b0bcf3
c3825-ipvoicek9-mz.124-7.bin IP VOICE	24328d8eabfc6c254da3b19a31c234ea
c3825-spservicesk9-mz.124-7.bin SP SERVICES	46b0c47a40bb32fd4b7be36d8e1f5359
c3845-adventerprisek9-mz.124-7.bin ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	fd30847f7489338c0bc7a3e081853ec3
c3845-adventerprisek9_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIPGW, TDMIP GW AES	8393476871591a3b7ccff1e883f0fe62
c3845-advipservicesk9-mz.124-7.bin ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	655d1dc18a1f6a1532fe22f1701c90f7
c3845-advsecurityk9-mz.124-7.bin ASK9-ASK9 FEAT SET FACTORY UPG FOR BUNDLES	a7eaf352d6b3cb49c38206f0dd06fbe7
c3845-entbasek9-mz.124-7.bin ENTERPRISE BASE	c7808841eb54568ee57f46556fcf0171
c3845-entservicesk9-mz.124-7.bin SPSK9-ESK9 FEAT SET FACTORY UPG FOR BUNDLES	a8ab969c21fcbeb90b0a71cffc6b088a
c3845-ipbasek9-mz.124-7.bin IP BASE	6e31deb3825ba3881aa8c1d2886cbeca
c3845-ipvoice_ivs-mz.124-7.bin INT VOICE/VIDEO, IPIP GW, TDMIP GW	6f9f4aa5f6760102f799b71b3e240382

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

Cisco IOS Image Name	MD5 Hash of Cisco IOS Image
c3845-ipvoicek9-mz.124-7.bin IP VOICE	fc3000c31ebac463d51779c62e075be7
c3845-spservicesk9-mz.124-7.bin SPSK9-SPSK9 FEAT SET FACTORY UPG FOR BUNDLES	f869c45b705cbe34b0c150c83dcfd28e
Cisco 7200 Series with Cisco IOS Release 12.4(7)	
c7200-c5ik9s-mz.124-7.bin BASE PDSN 3DES	7dac21461b43d4d82404664958590420
c7200-c5is-mz.124-7.bin BASE PDSN UPGRADE	12d02c6df7ce82821061aa9d52e96370
c7200-c6ik9s-mz.124-7.bin ENH PDSN UPGRADE TO 3DES	b997fe3218682cfbad211f7f8a1c057b
c7200-c6is-mz.124-7.bin ENHANCED PDSN	d52a28f8632c8ee472e011be2e2fe504
c7200-g4js-mz.124-7.bin ENTERPRISE SSG	e8ea07c80860f2507aeaddae36e10fb3
c7200-g6ik8s-mz.124-7.bin GGSN 4.0 (IPSEC)	2c2e64b2222b6aedba1e07b367add124
c7200-g6ik9s-mz.124-7.bin UPGRADE FROM 3.0 TO 4.0 (3DES)	45cac95a201e2d51d008d7fe3b36b0e3
c7200-g6is-mz.124-7.bin UPGRADE FROM 1.4 TO 4.0 (BASE)	f768a3ee5cdb57e62b6e7e50bd14876c
c7200-h1ik9s-mz.124-7.bin MW HOME AGENT 3DES	0592503927beeb11bcedc33bff0c876f
c7200-h1is-mz.124-7.bin MW HOME AGENT	6258506afb30df11a760bccd9f3f5946
c7200-ik9o3s-mz.124-7.bin IP/FW/IDS IPSEC 3DES	479c1dbdabfbfd323dbabeec60bb2c37
c7200-ik9s-mz.124-7.bin IP IPSEC 3DES	7f8436785f43184b817c7fc24550d442
c7200-ik9su2-mz.124-7.bin IP IPSEC 3DES LAWFUL INTERCEPT	5b7c585ef09ac19768d3126e3ad24ec8
c7200-is-mz.124-7.bin IP	e88bd10bd6e4e1ec5a90cce3a3d5db43
c7200-jk9o3s-mz.124-7.bin ENTERPRISE/FW/IDS IPSEC 3DES	c2219e7cbfaf615a66893d011836a059
c7200-jk9s-mz.124-7.bin ENTERPRISE IPSEC 3DES	e160877838802b878babf6292bd3e317
c7200-js-mz.124-7.bin ENTERPRISE	3c2b5e882dba6aa52a2c4a232dfde314
c7200-kboot-mz.124-7.bin BOOT IMAGE(ON/I/O CARD W/GE OR 2FE/E)	3a1c93e5c0fd7f153ef56779977f1236

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

Cisco IOS Image Name	MD5 Hash of Cisco IOS Image
c7200-p-mz.124-7.bin SERVICE PROVIDER	84812e995b5db025cef4da0a22d26687
c7200-pk9u2-mz.124-7.bin SERVICE PROVIDER IPSEC 3DES LAWFUL INTERCEPT	015067549bbbcdde10abac8ce9f8b607
Cisco 7300 Series with Cisco IOS Release 12.4(7)	
c7301-boot-mz.124-7.bin BOOTLOADER	d0bd3e075bc4fda8957654045855edf4
c7301-g4js-mz.124-7.bin ENTERPRISE SSG	f2cc374759c7333b78bdb889fb52045b
c7301-ik9o3s-mz.124-7.bin IP/FW/IDS IPSEC 3DES	d0f7a01a8411310035fea24432d559ee
c7301-ik9s-mz.124-7.bin IP PLUS IPSEC 3DES	d0b037b930b66b240bc685931834efe1
c7301-ik9su2-mz.124-7.bin IP PLUS IPSEC 3DES LAWFUL INTERCEPT	a028972757ce2f89ff4f12a67d786f44
c7301-is-mz.124-7.bin IP	939a7db31609fec3dfd5991975c98a6b
c7301-jk9o3s-mz.124-7.bin ENTERPRISE/FW/IDS IPSEC 3DES	667fda94a7eed9dd618c626fff456524
c7301-jk9s-mz.124-7.bin ENTERPRISE PLUS IPSEC 3DES	67af0528dfb8da46ff1f7d586a74a29c
c7301-jk9su2-mz.124-7.bin ENTERPRISE PLUS LAWFUL INTERCEPT IPSEC 3DES	b3a48b9d50e693ee717f4854ea17dead
c7301-js-mz.124-7.bin ENTERPRISE	fa63ecaeffa90f68c96f10e9c113248b
c7301-p-mz.124-7.bin SERVICE PROVIDER	c8ebf743207ff0b68fbfe1b3f5019572
c7301-pk9u2-mz.124-7.bin SERVICE PROVIDER IPSEC 3DES LAWFUL INTERCEPT	a0fc89e6546b0e250d6d8acc26c4a470
Cisco 7600 or Cisco 6500 with Cisco IOS Release 12.2(33)SRA	
s72033-adventerprisek9_wan-mz.122-33.SRA.bin ADVANCED ENTERPRISE SERVICES SSH	daf02dfde746c842844aa57dafb68a7b

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 12.4:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/index.htm

Documentation for Cisco IOS Release 12.2SR:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/index.htm

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

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/web/ordering/root/index.html

- 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.

Note This document is to be used in conjunction with the documents listed in the section "Related Documentation."