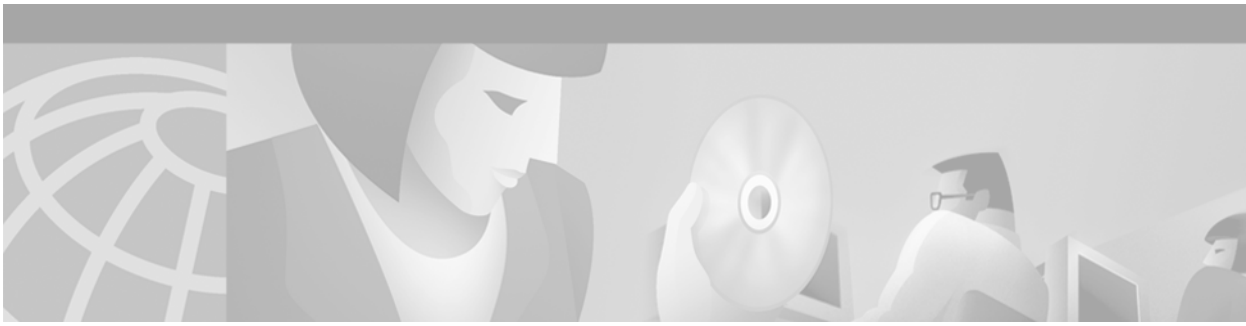


Cisco 2691 Modular Access Router FIPS 140-2 Non-Proprietary Security Policy

Introduction

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 2691 router. This security policy describes how the Cisco 2691 router meets the security requirements of FIPS 140-2, and how to operate the Cisco 2691 router in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 certification of the Cisco 2691 router.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

This document contains the following sections:

References

This document deals only with operations and capabilities of the Cisco 2691 router in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Cisco 2691 router and the entire Cisco 2600 series from the following sources:

CISCO SYSTEMS

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

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The Cisco 2600 series product descriptions can be found at:

  http://www.cisco.com/en/US/products/hw/routers/ps259/index.html
- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module

Terminology

In this document, the Cisco 2691 router is referred to as the router, the module, or the system.

Document Organization

The Security Policy document is part of the complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Cisco 2691 router and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the Cisco 2691 router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Certification Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

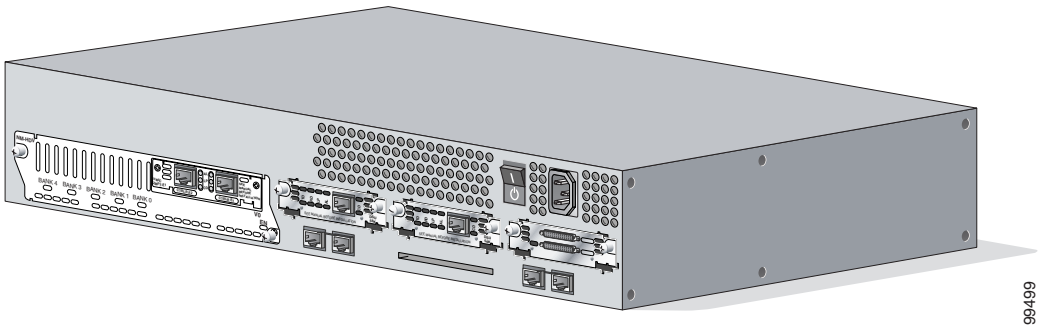
The Cisco 2691 Router

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Cisco 2691 modular multi-service router offers versatility, integration, and security to branch offices. With over 100 Network Modules and WAN Interface Cards (WICs), the modular architecture of the Cisco router easily allows interfaces to be upgraded to accommodate network expansion. The Cisco 2691 provides a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the Cisco 2691 router.

Note The MTU size for the NM-1GE module cannot be set to support jumbo frames on the Cisco 2691 router.

The Cisco 2691 Cryptographic Module

Figure 1 The Cisco 2691 Router



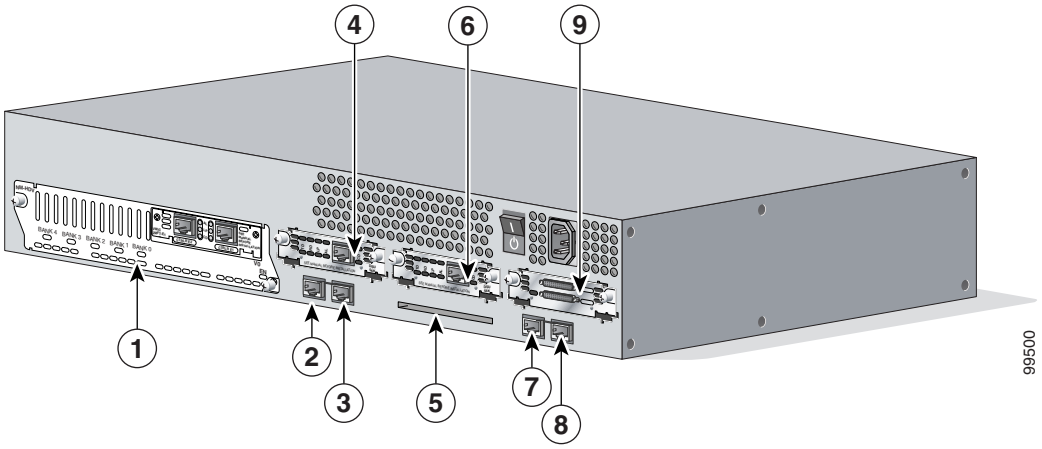
The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case; all portions of the “backplane” of the case which are not designed to accommodate a WIC or Network Module; and the inverse of the three-dimensional space within the case that would be occupied by an installed WIC or Network Module. The cryptographic boundary includes the connection apparatus between the WIC or Network Module and the motherboard/daughterboard that hosts the WIC or Network Module, but the boundary does not include the WIC or Network Module itself. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular WICs or Network Modules. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

Cisco IOS features such as tunneling, data encryption, and termination of Remote Access WANs via IPSec, Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocols (L2TP) make the Cisco 2600 an ideal platform for building virtual private networks or outsourced dial solutions. Cisco 2600 series’ RISC-based processor provides the power needed for the dynamic requirements of the remote branch office, achieving wire speed Ethernet to Ethernet routing with up to 70 thousand packets per second (Kpps) throughput capacity.

Module Interfaces

The interfaces for the router are located on the rear panel as shown in Figure 2.

Figure 2 Cisco 2691 Physical Interfaces



The Cisco 2691 router features console and auxiliary ports, dual fixed LAN interfaces, a Network Module slot, two Cisco WAN interface card (WIC) slots, and a Compact Flash slot.

LAN support includes single and dual Ethernet options; 10/100 Mbps auto-sensing Ethernet; mixed Token-Ring and Ethernet; and single Token Ring chassis versions. WAN interface cards support a variety of serial, ISDN BRI, and integrated CSU/DSU options for primary and backup WAN connectivity, while available Network Modules support multi-service voice/data/fax integration, departmental dial concentration, and high-density serial options. The AIM slot supports integration of advanced services such as hardware-assisted data compression and encryption. All Cisco 2600 series routers include an auxiliary port supporting 115Kbps Dial-On-Demand Routing, ideal for back-up WAN connectivity.

When a Network Module is inserted, it fits into an adapter called the Network Module expansion bus. The expansion bus interacts with the PCI bridge in the same way that the fixed LAN ports do; therefore, no critical security parameters pass through the Network Module (just as they don't pass through the LAN ports). Network modules do not perform any cryptographic functions.

WICs are similar to Network Modules in that they greatly increase the router's flexibility. A WIC is inserted into one of two slots, which are located above the fixed LAN ports. WICs interface directly with the processor. They do not interface with the cryptographic card; therefore no security parameters will pass through them. WICs cannot perform cryptographic functions; they only serve as a data input and data output physical interface.

The physical interfaces include a power plug for the power supply and a power switch. The router has two Fast Ethernet (10/100 RJ-45) connectors for data transfers in and out. The module also has two other RJ-45 connectors on the back panel for a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem. The 10/100Base-T LAN ports have Link/Activity, 10/100Mbps, and half/full duplex LEDs. Figure 3 shows the LEDs located on the rear panel with descriptions detailed in Table 1:

Figure 3 Cisco 2691 Rear Panel LEDs

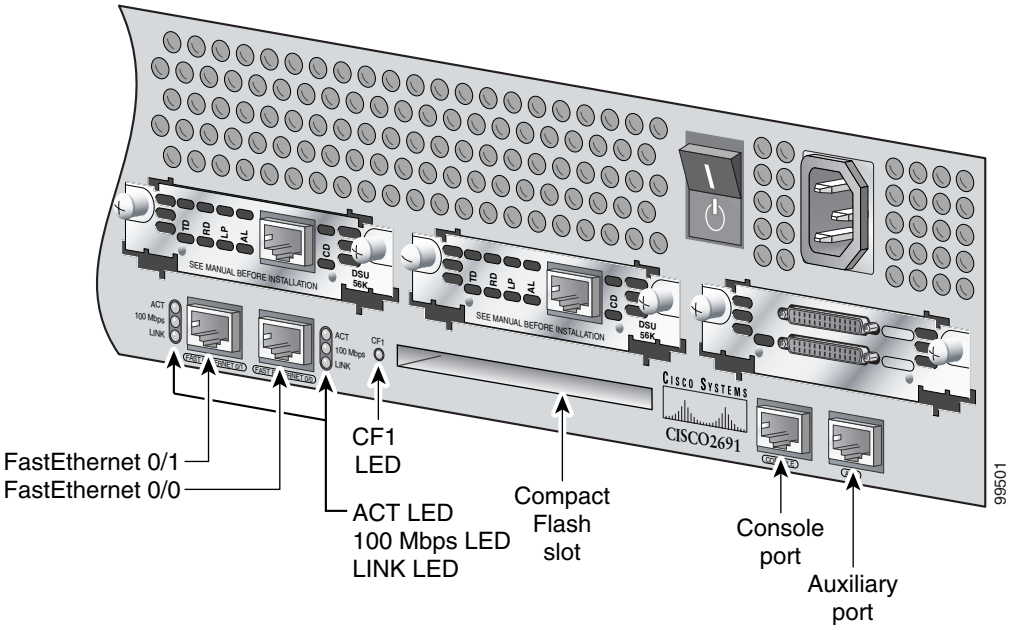


Table 1 Cisco 2691 Rear Panel LEDs and Descriptions

LED	Indication	Description
LINK	On	An Ethernet link has been established
	Off	No Ethernet link established
ACT	On	The interface is transmitting or receiving packets
	Off	The interface is not transmitting or receiving packets
100 Mbps	On	The speed of the interface is 100 Mbps
	Off	The speed of the interface is 10 Mbps or no link is established
CF1	On	The Flash device is being accessed in either READ or WRITE mode
	Off	The Flash device is not being accessed

Figure 4 shows the front panel LEDs, which provide overall status of the router's operation. The front panel displays whether or not the router is booted, if the redundant power is (successfully) attached and operational, and overall activity/link status.

Figure 4 Cisco 2691 Front Panel LEDs

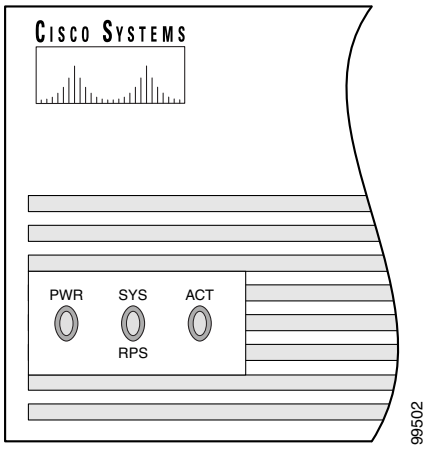


Table 2 provides more detailed information conveyed by the LEDs on the front panel of the router:

Table 2 Cisco 2691 Front Panel LEDs and Descriptions

LED	Indication	Description
PWR	On	Power is supplied to the router
	Off	The router is not powered on
SYS/RPS	Rapid blinking	System is booting
	Slow blinking	System error
	On	System OK
ACT	Off	No system activity
	Blinking	System activity

All of these physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in Table 3:

Table 3 FIPS 140-2 Logical Interfaces

Router Physical Interface	FIPS 140-2 Logical Interface
10/100BASE-TX LAN Port WIC Interface Network Module Interface Console Port Auxiliary Port Compact Flash slot	Data Input Interface
10/100BASE-TX LAN Port WIC Interface Network Module Interface Console Port Auxiliary Port Compact Flash slot	Data Output Interface

Table 3 FIPS 140-2 Logical Interfaces (continued)

Router Physical Interface	FIPS 140-2 Logical Interface
10/100BASE-TX LAN Port WIC Interface Network Module Interface Power Switch Console Port Auxiliary Port	Control Input Interface
10/100BASE-TX LAN Port WIC Interface Network Module Interface LAN Port LEDs 10/100BASE-TX LAN Port LEDs Power LED Activity LED Console Port Auxiliary Port	Status Output Interface
Power Plug	Power Interface

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authentication. A complete description of all the management and configuration capabilities of the Cisco 2691 Router can be found in the Performing Basic System Management manual and in the online help for the router.

Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the “enable” password) is defined. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the router**—define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**—create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions**—view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- **Manage the router**—log off users, shutdown or reload the outer, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.

- **Set Encryption/Bypass**—set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- **Change Network Modules**—insert and remove modules in the Network Module slot as described in Section 3.1, Number 2 of this document.
- **Change WAN Interface Cards**—insert and remove WICs in the WAN interface slot as described in Section 3.1, Number 3 of this document.

User Services

A User enters the system by accessing the console port with a terminal program. The Cisco IOS prompts the User for their password. If the password is correct, the User is allowed entry to the Cisco IOS executive program. The services available to the User role consist of the following:

- **Status Functions**—view state of interfaces, state of layer 2 protocols, version of Cisco IOS currently running
- **Network Functions**—connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace)
- **Terminal Functions**—adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services**—display directory of files kept in flash memory

Physical Security

The router is entirely encased by a thick steel chassis. The rear of the unit provides 1 Network Module slot, 3 WIC slots, on-board LAN connectors, Console/Auxiliary connectors, Compact Flash slot, the power cable connection and a power switch. The top portion of the chassis may be removed to allow access to the motherboard, memory, and expansion slots.

Once the router has been configured in to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

Step 1 Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10°C.

Step 2 Place the first label on the router as shown in Figure 5. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the right side of the router. Any attempt to remove the enclosure will leave tamper evidence.

Step 3 Place the second label on the router as shown in Figure 5. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the left side of the router. Any attempt to remove the enclosure will leave tamper evidence.

Step 4 Place the third label on the router as shown in Figure 5. The tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the Network Module slot. Any attempt to remove a Network Module will leave tamper evidence.

Step 5 Place the fourth label on the router as shown in Figure 5. The tamper evidence label should be placed so that the half of the label covers the enclosure and the other half covers the left WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

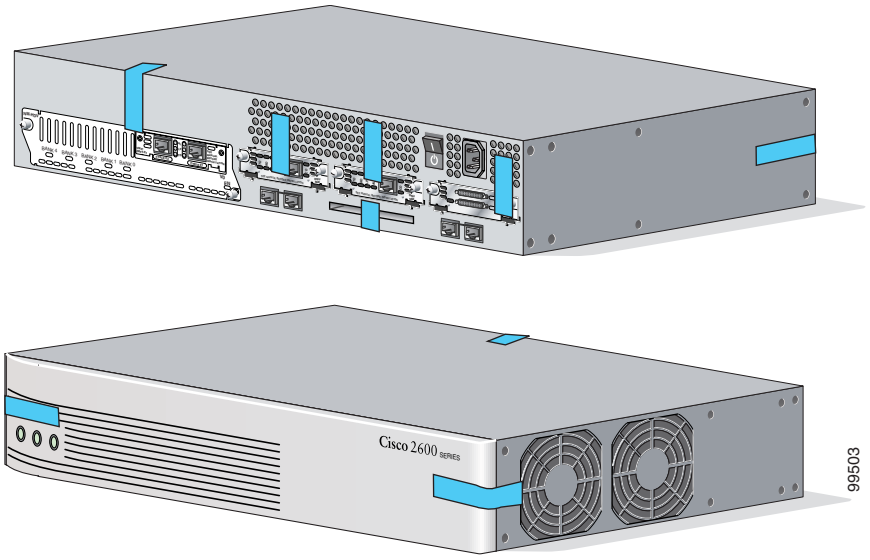
Step 6 Place the fifth label on the router as shown in Figure 5. The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the middle WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

Step 7 Place the sixth label on the router as shown in Figure 5. The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the right WAN interface card slot. Any attempt to remove a WAN interface card will leave tamper evidence.

Step 8 Place the seventh label on the router as shown in Figure 5. The tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the Compact Flash slot. Any attempt to remove a CF card will leave tamper evidence.

The labels completely cure within five minutes.

Figure 5 Tamper Evidence Label Placement



The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router, remove Network Modules or WIC cards, or the front faceplate will damage the tamper evidence seals or the painted surface and metal of the module cover. Since the tamper evidence seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word “Opened” may appear if the label was peeled back.

Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. Keys are also password protected and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange or Internet Key Exchange (IKE).

The module contains a cryptographic accelerator card, which provides AES (128-bit), DES (56-bit), and 3DES (168-bit) IPSec encryption at up to 90Mbps (3DES, 96Mbps DES), MD5 and SHA-1 hashing, and has hardware support for DH and RSA key generation.

The module supports the following keys (critical security parameters):

- IPSEC Session
- IKE Key-pairs
- IKE Public
- Pre-shared
- DH Key-pairs
- X9.17 PRNG Seed Key

The module supports DES, 3DES, SHA-1, MD-5, MD-4, SHA-1 HMAC, MD5 HMAC, Diffie-Hellman, RSA (for digital signatures and encryption), and AES cryptographic algorithms. The MD-5, MD-5 HMAC, MD-4, and RSA encryption algorithms are disabled when operating in FIPS mode.

The module supports three types of key management schemes:

- Manual key exchange method that is symmetric. DES/3DES/AES key and HMAC-SHA key are exchanged manually and entered electronically.
- Internet Key Exchange method with support for exchanging pre-shared keys manually and entering electronically.
  - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, 3DES or AES keys.
  - The pre-shared key is also used to derive HMAC-SHA key.
- Internet Key Exchange with RSA-signature authentication.

The module supports commercially available methods of key establishment, including Diffie-Hellman and IKE. See the Configuring IPSec Network Security document, Submission Document 7A, and the Internet Key Exchange Security Protocol Commands, Submission Document 7B.

All pre-shared keys are associated with a password of the role that created the keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol.

Key Zeroization:

Each key can be zeroized by sending the “no” command prior to the key function commands. This will zeroize each key from the DRAM, which is a running configuration. The Crypto Officer must copy the running configuration (DRAM) to the start-up configuration (NVRAM) in order to completely zeroize the keys. Additionally, the Crypto Officer can zeroize all operator passwords by overwriting them with spaces or by deleting the operators' access.

“Clear Crypto IPSec SA” will zeroize the DES session key (which is derived using the Diffie-Hellman key agreement technique) from the DRAM. This session key is only available in the DRAM; therefore this command will completely zeroize this key. The following command will zeroize the manual keys from the DRAM:

- `no set session-key inbound ah spi hex-key-data`
- `no set session-key outbound ah spi hex-key-data`
- `no set session-key inbound esp spi cipher hex-key-data [authenticator hex-key-data]`
- `no set session-key outbound esp spi cipher hex-key-data [authenticator hex-key-data]`

The DRAM running configuration must be copied to the start-up configuration in NVRAM in order to completely zeroize the keys.

The following commands will zeroize the pre-shared keys from the DRAM:

- `no crypto isakmp key key-string address peer-address`
- `no crypto isakmp key key-string hostname peer-hostname`

The DRAM running configuration must be copied to the start-up configuration in NVRAM in order to completely zeroize the keys.

Self-Tests

In order to prevent any secure data being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations.

If any of these self-tests fail, the router will transition into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Power Up Tests

The self-test run at power-up includes a cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (AES, DES, 3DES), on the message digest (SHA-1) and on the Diffie-Hellman algorithm. Also performed at startup are a software integrity test using an EDC, and a set of Statistical Random Number Generator (RNG) tests.

Conditional Tests

The following tests are also run periodically or conditionally: a Bypass Mode test performed conditionally prior to executing IPSec, and the continuous random number generator test.

Secure Operation of the Cisco 2691 Router

The Cisco 2691 router meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

Initial Setup

- The Crypto Officer must apply tamper evidence labels as described in Section 2.4 of this document.
- Only a Crypto Officer may add and remove Network Modules. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in Section 2.4, Item 4.
- Only a Crypto Officer may add and remove WAN Interface Cards. When removing the tamper evidence label, the Crypto Officer should remove the entire label from the router and clean the cover of any grease, dirt, or oil with an alcohol-based cleaning pad. The Crypto Officer must re-apply tamper evidence labels on the router as described in Section 2.4, Item 5 and/or Item 6.

System Initialization and Configuration

- The Crypto Officer must perform the initial configuration. Cisco IOS version 12.3(3a) is the only allowable image; no other image may be loaded.
- The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically boots the Cisco IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

  ```
  config-register 0x0101
  ```

- The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

  ```
  enable secret <PASSWORD>
  ```

- The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

  ```
  line con 0
  password <PASSWORD>
  login local
  ```

- The Crypto Officer shall only assign users to a privilege level 1 (the default).
- The Crypto Officer shall not assign a command to any privilege level other than its default.

IPSec Requirements and Cryptographic Algorithms

- There are two types of key management method that are allowed in FIPS mode: Internet Key Exchange (IKE) and IPSec manually entered keys.
- Although the Cisco IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
  - ah-sha-hmac
  - esp-des
  - esp-sha-hmac
  - esp-3des
  - esp-aes
- The following algorithms are not FIPS approved and should be disabled:
  - RSA for encryption
  - MD-4 and MD-5 for signing
  - MD-5 HMAC

Protocols

SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, only gets are allowed under SNMP v2C.

Remote Access

- Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.
- SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms.

Related Documentation

For more information about the Cisco 2691 modular access router, refer to the following documents:

- *Cisco 2600 Series Modular Routers Quick Start Guide*
- *Cisco 2600 Series Hardware Installation Guide*
- *Software Configuration Guide for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

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