FIPS 140-2 Nonproprietary Security Policy for Cisco 7206VXR NPE-G1 Router with Single or Dual VPN Acceleration Module 2 (VAM2)

Introduction

This security policy describes how the Cisco 7206VXR router with a NPE-G1 processor and the VPN Acceleration Module 2 (VAM2) (Hardware Version:7206 VXR; NPE-G1:Hardware Version 1.1, Fab Version 05; VAM2:Hardware Version 2.0, Board Version A0; Firmware Version:IOS 12.3(3d)) meets the security requirements of FIPS 140-2. This document also includes instructions for installing the Cisco 7206VXR with the VAM2 in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

Note This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on the last page.

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 includes the following sections:

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

FIPS 140-2 Submission Package

This Security Policy document is one item in the FIPS 140-2 Submission Package. In addition to this document, the Submission Package includes:

- Vendor evidence document
- Finite state machine
- Module software listing
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, contact Cisco Systems, Inc. See "Obtaining Technical Assistance" section on page 19.

Overview

Cisco 7206VXR routers support gigabit capabilities to improve data, voice, and video integration in both the service provider and enterprise environments. Cisco 7206VXR routers support a high-speed network services engine (NSE), the high-speed network processing engine (NPE-G1), and other network processing engines.

Cisco 7206VXR routers accommodate a variety of network interface port adapters and an Input/Output (I/O) controller. A Cisco 7206VXR router equipped with an NPE-G1 supports up to six high-speed port adapters and higher-speed port adapter interfaces including Gigabit Ethernet and OC-12 ATM (Optical Carrier-12 Asynchronous Transfer Mode). Cisco 7206VXR routers accommodate up to two AC-input or DC-input power supplies.

Cisco 7206VXR routers support the following features:

- Online insertion and removal (OIR)—Adds, replaces, or removes port adapters without interrupting the system.
- Dual hot-swappable, load-sharing power supplies—Provides system power redundancy; if one power supply or power source fails, the other power supply maintains system power without interruption. Also, when one power supply is powered off and removed from the router, the second power supply immediately takes over the router power requirements without interrupting normal operation of the router.
- Environmental monitoring and reporting functions—Maintains normal system operation by resolving adverse environmental conditions prior to loss of operation.
- Downloadable software—Loads new images into Flash memory remotely, without having to physically access the router.

The Cisco 7206VXR router incorporates either one or two VPN Acceleration Module 2 (VAM2) cryptographic accelerator cards. The VAM2s are installed in port adapter slots. The VPN Acceleration Module 2 (VAM2) is a single-width acceleration module that provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The VAM2 off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

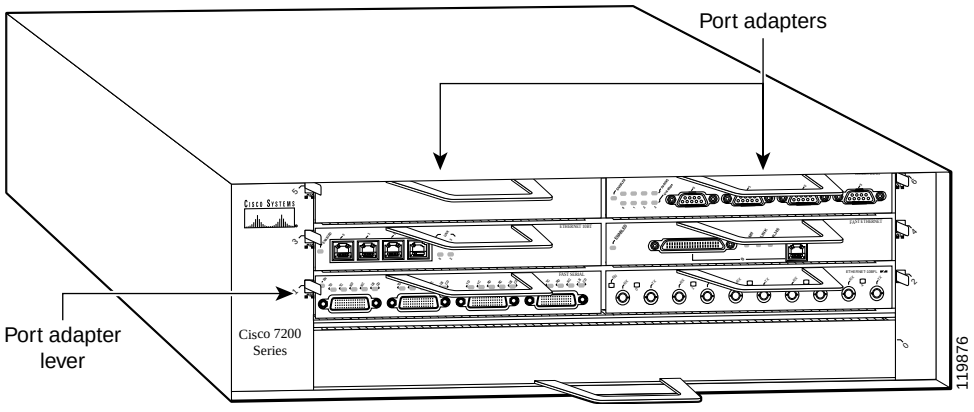
Cryptographic Module

The Cisco 7206VXR NPE-G1 router with a single VPN Acceleration Module 2 (VAM2) or dual VPN Acceleration Module 2 (VAM2) supports multi-protocol routing and bridging with a variety of protocols and port adapter combinations available for Cisco 7200 series routers. The metal casing that fully encloses the module establishes the cryptographic boundary for the router, all the functionality discussed in this document is provided by components within the casing. The Cisco 7206VXR has six slots for port adapters, one slot for an I/O controller, and one slot for a network processing engine or network services engine. The router with single or dual VAM2 is a multi-chip standalone cryptographic module.

The following defines the configuration tested for the Cisco 7206VXR:

- Cisco 7206VXR chassis
- Network Processing Engine (NPE-G1)
- VAM2 hardware acceleration card (single and dual)
- One power supply

Figure 1 Cisco 7206VXR NPE-G1 Router (Front View)



The NPE-G1 uses an RM7000 microprocessor that operates at an internal clock speed of 350 MHz. The NPE-G1 uses SDRAM for storing all packets received or sent from network interfaces. The SDRAM memory array in the system allows concurrent access by port adapters and the processor. The NPE-G1 has three levels of cache: a primary and a secondary cache that are internal to the microprocessor, and a tertiary 4-MB external cache that provides additional high-speed storage for data and instructions.

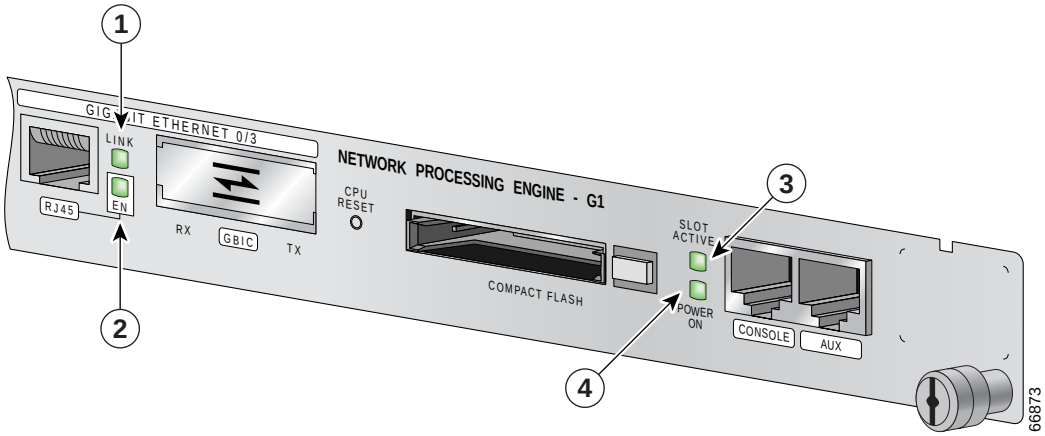
The Cisco 7206VXR router comes equipped with one 280W AC-input power supply. A 280W DC -input power supply option is also available. A power supply filler plate is installed over the second power supply bay. A fully configured Cisco 7206VXR router operates with only one installed power supply; however, a second, optional power supply of the same type provides hot-swappable, load-sharing, redundant power.

Module Interfaces

The router interfaces are located on the rear panel. The module has three interfaces, each with 2 ports: one Fast Ethernet/Gigabit (10/100/1000 RJ-45) connector and one Gigabit Ethernet port; only one of these two ports can be active for each interface. The module also has a compact flash interface, reset switch, and two other RJ-45 connectors for a console terminal for local system access and an auxiliary port for remote system access or dial backup using a modem.

Figure 2 shows the front panel LEDs (light emitting diodes), which shows overall status of the router operation. The front panel displays whether or not the router is booted, if the redundant power is attached and operational, and the overall activity/link status.

Figure 2 Cisco 7206VXR Router Front Panel LEDs

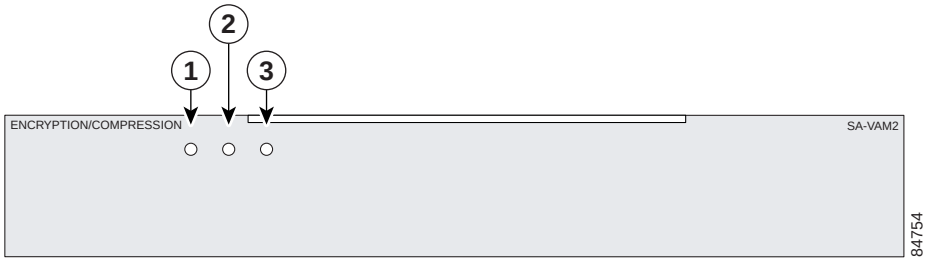


Callout	LED	Indication	Description
1	Enabled	Green	The NPE-G1 faceplate LEDs indicate system and port status. The RJ-45 and GBIC ports share the same LINK LED because only one of these ports per interface (0/1, 0/2, or 0/3) can be used at any one time. The EN (enable) LED is on if the RJ-45 port is in use.
		Off	No traffic is transgressed.
2	EN (enabled)	Green	The RJ-45 port is active
		Off	The Gigabit Ethernet port is active

Callout	LED	Indication	Description
3	Slot active	Green	Compact flash interface is active
		Off	The compact flash interface is inactive
4	Power On	Green	The POWER ON LED is on whether or not an I/O controller is present in the router. The compact Flash Disk slot can be used whether or not an I/O controller is present in the router. The SLOT ACTIVE LED is on only when the compact Flash Disk slot is in use.
		Off	The module is not powered on

The VAM2 has three LEDs, as shown in Figure 3.

Figure 3 VAM2 LEDs



Number	LED Label	Color	State	Function
1	ENABLE	Green	On	Indicates the VAM2 is powered up and enabled for operation.
2	BOOT	Amber	Pulses	Indicates the VAM2 is operating.
			On	Indicates the VAM2 is booting or a packet is being encrypted or decrypted.
3	ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.

All physical interfaces are separated into the logical interfaces from FIPS as shown in Table 1

Table 1 FIPS 140-2 Logical Interface

Router Physical Interface	FIPS 140-2 Logical Interface
10/100/1000 BASE-TX LAN Port Gigabit Ethernet Port Port Adapter Interface Console Port Auxiliary Port PCMCIA Slot	Data Input Interface
10/100/1000 BASE-TX LAN Port Gigabit Ethernet Port Port Adapter Interface Console Port Auxiliary Port PCMCIA Slot	Data Output Interface
10/100/1000 BASE-TX LAN Port Gigabit Ethernet Port Power Switch Reset Switch Console Port Auxiliary Port	Control Input Interface

Table 1 FIPS 140-2 Logical Interface (Continued)

Router Physical Interface	FIPS 140-2 Logical Interface
10/100/1000BASE-TX LAN Port LEDs Gigabit Ethernet Port Enabled LED PCMCIA LEDs IO Pwr Ok LED VAM2 LEDs Console Port Auxiliary Port	Status Output Interface
Power Plug	Power Interface

In addition to the built-in interfaces, the router also has additional port adapters that can optionally be placed in an available slot. These port adapters have many embodiments, including multiple Ethernet, token ring, and modem cards to handle frame relay, ATM, and ISDN (Integrated Services Digital Network) connections. (Note: These additional port adapters were excluded from this FIPS 140-2 Validation.)

Roles and Services

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 to configure and maintain the router using Crypto Officer services, while Users exercise only the basic User services. Both roles are authenticated by providing a valid username and password. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode. See the *Cisco 7206VXR Installation and Configuration Guide* for more configuration information.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See the "Secure Operation" section on page 17 for more information. If only integers 0-9 are used without repetition for an 8 digit PIN, the probability of randomly guessing the correct sequence is 1 in 1,814,400. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

Crypto Officer Role

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer assigns 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:

- Configures the Router: Defines network interfaces and settings, creates command aliases, sets the protocols the router will support, enables interfaces and network services, sets system date and time, and loads authentication information.
- Defines Rules and Filters: Creates 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: Views the router configuration, routing tables, active sessions; views SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics; reviews accounting logs, and views physical interface status.
- Manages the Router: Logs off users, shuts down or reloads the router, manually backs up router configurations, views complete configurations, manager user rights, and restores router configurations.
- Sets Encryption/Bypass: Sets up the configuration tables for IP tunneling; sets keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- Changes Port Adapters: Inserts and removes adapters in a port adapter slot.

User Role

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

- Status Functions: Views state of interfaces, state of layer 2 protocols, and version of IOS currently running
- Network Functions: Connects to other network devices (via outgoing telnet or PPP) and initiates diagnostic network services (i.e., ping, mtrace)
- Terminal Functions: Adjusts the terminal session (e.g., lock the terminal, adjust flow control)
- Directory Services: Displays directory of files kept in flash memory

Physical Security

The router is encased in a steel chassis. The front of the router includes six port adapter slots. The rear of the router includes on-board LAN connectors, PC Card slots, and Console/Auxiliary connectors, power cable connection, a power switch, and access to the Network Processing Engine.

Any port adapter slot not populated with a port adapter must be populated with a slot cover (blank port adapter) to operate in FIPS compliant mode. Slot covers are included with each router; additional covers may be ordered from Cisco. You apply the same procedure for labeling port adapters covers as for the port adapters.

Once the router has been configured to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. The word ‘Open’ may appear on the label if it was peeled away from the surface of the module. The Crypto Officer should be instructed to record serial numbers, and to inspect for signs of tampering or changed numbers periodically.

To seal the system, apply serialized tamper-evidence labels as described below, and as shown in Figure 4 and Figure 5:

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 ambient air must be above 10C, otherwise the labels may not properly cure.

Step 2 A tamper evidence label should be placed so that the one half of the label covers the enclosure and the other half covers the NPE-G1.

Step 3 A tamper evidence label should be placed over the Flash PC Card slot on the NPE-G1.

Step 4 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 1.

Step 5 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 2.

Step 6 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 3.

Step 7 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 4.

Step 8 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 5.

Step 9 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the port adapter slot 6.

Step 10 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the I/O Controller blank face plate.

Step 11 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the power supply plate.

Step 12 A tamper evidence label should be placed so that one half of the label covers the enclosure and the other half covers the redundant power supply plate.

Step 13 Allow the labels to cure for five minutes.

Figure 4 Tamper Evidence Label Placement (Front View)

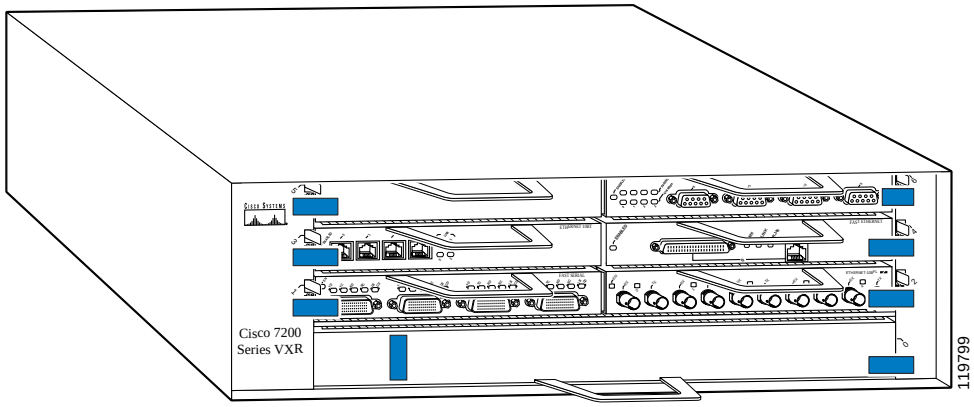
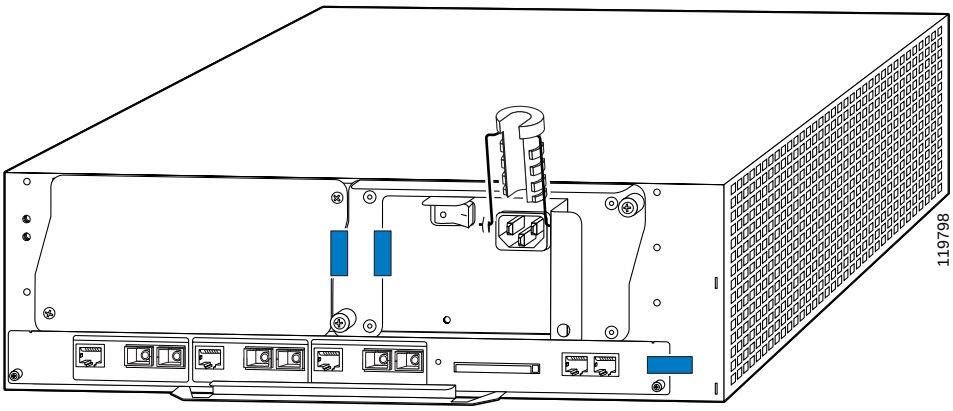


Figure 5 Tamper Evidence Label Placement (Rear View)



Cryptographic Key Management

The IOS software implementations of the FIPS algorithms have the following FIPS algorithm certifications:

- DES (certificate #202)
- 3DES (certificate #156)
- AES (certificate #46)
- SHA-1 (certificate #26)
- SHA-1 HMAC (vendor affirmed)

The VAM2 firmware implementations of the FIPS algorithms have the following FIPS algorithm certifications:

- DES (certificate #204)
- 3DES (certificate #158)
- AES (certificate #48)
- SHA-1 (certificate #143)
- SHA-1 HMAC (vendor affirmed)

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 stored within the module. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys are exchanged manually and entered electronically via manual key exchange methods or Internet Key Exchange (IKE) as described below.

The modules contain a cryptographic accelerator card (the VAM2), which provides AES, DES (56-bit) (only for legacy systems), and 3DES (168-bit) IPSec encryption, MD5 and SHA-1 hashing, HMAC-SHA-1, RSA (sign and verify), and has hardware support for Diffie-Hellman (DH) and RSA key generation.

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

Table 2 Critical Security Parameters

#	CSP Name	Description	Storage
1	CSP 1	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	DRAM (plaintext)
2	CSP2	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
3	CSP3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
4	CSP4	Same as above	DRAM (plaintext)
5	CSP5	Same as above	DRAM (plaintext)
6	CSP6	Same as above	DRAM (plaintext)
7	CSP7	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
8	CSP8	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
9	CSP9	The RSA private key. “crypto key zeroize” command zeroizes this key.	NVRAM (plaintext)
10	CSP10	The key used to generate IKE skeyid during preshared-key authentication. The **no crypto isakmp key** command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)
11	CSP11	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
12	CSP12	The RSA public key used to validate signatures within IKE. These keys are expired either when CRL (certificate revocation list) expires or 5 secs after if no CRL exists. After above expiration happens and before a new public key structure is created this key is deleted. This key does not need to be zeroized because it is a public key; however, it is zeroized as mentioned here.	DRAM (plaintext)
13	CSP13	The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash.	NVRAM (plaintext)

Table 2 Critical Security Parameters (Continued)

#	CSP Name	Description	Storage
14	CSP14	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
15	CSP15	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
16	CSP16	The RSA public key of the CA. The **no crypto ca trust** <*label*> command invalidates the key and it frees the public key label which in essence prevent use of the key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
17	CSP17	This key is a public key of the DNS server. Zeroized using the same mechanism as above. The **no crypto ca trust** <*label*> command invalidates the DNS server public key and it frees the public key label which in essence prevent use of that key. This label is different from the label in the above key. This key does not need to be zeroized because it is a public key.	NVRAM (plaintext)
18	CSP18	The SSL session key. Zeroized when the SSL connection is terminated.	DRAM (plaintext)
19	CSP19	The ARAP key that is hardcoded in the module binary image. This key can be deleted by erasing the Flash.	Flash (plaintext)
20	CSP20	This is an ARAP user password used as an authentication key. A function uses this key in a DES algorithm for authentication.	DRAM (plaintext)
21	CSP21	The key used to encrypt values of the configuration file. This key is zeroized when the **no key config-key** command is issued.	NVRAM (plaintext)
22	CSP22	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM (plaintext)
23	CSP23	The RSA public key used in SSH. Zeroized after the termination of the SSH session. This key does not need to be zeroized because it is a public key; However, it is zeroized as mentioned here.	DRAM (plaintext)
24	CSP24	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)

Table 2 Critical Security Parameters (Continued)

#	CSP Name	Description	Storage
25	CSP25	This key is used by the router to authenticate itself to the peer. The key is identical to #22 except that it is retrieved from the local database (on the router itself). Issuing the **no username password** command zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
26	CSP26	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
27	CSP27	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
28	CSP28	The plaintext password of the Crypto Officer role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
29	CSP29	The ciphertext password of the Crypto Officer role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
30	CSP30	The RADIUS shared secret. This shared secret is zeroized by executing the “no” form of the RADIUS shared secret set command.	DRAM (plaintext), NVRAM (plaintext)
31	CSP31	The TACACS+ shared secret. This shared secret is zeroized by executing the “no” form of the TACACS+ shared secret set command.	DRAM (plaintext), NVRAM (plaintext)
32	CSP32	The keys and CSPs above from no. The CSP from 1 to 31 are located in the router outside from VAM2. However, the CSP 32 object is located in the RAM of the VAM2. All key objects of the VAM2 are built upon the CSP 32 object. The destructor of the CSP 32 object uses memset function to overwrite all bytes of the object to 0x00.	DRAM of VAM2 (plaintext)

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Figure 6.

Figure 6 Role and Service Access to CSPs

SRDI/Role/Service Access Policy	Data Security Item Relevant	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16
Role/Service																	
User role																	
Status Functions																	
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Terminal Functions																	
Directory Services																	
Crypto-Officer Role																	
Configure the Router														rwd			
Define Rules and Filters																	
Status Functions																	
Manage the Router		d															
Set Encryption/Bypass		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd		rwd	rwd	rw
Change Port Adapters																	

SRDI/Role/Service Access Policy	Data Security Item Relevant	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22	CSP 23	CSP 24	CSP 25	CSP 26	CSP 27	CSP 28	CSP 29	CSP 30	CSP 31	CSP 32
Role/Service																	
User role																	
Status Functions																	
Network Functions		r	r	r	r		r	r	r	r	r	r					
Terminal Functions																	
Directory Services																	
Crypto-Officer Role																	
Configure the Router				rwd		rwd				rwd							
Define Rules and Filters																	
Status Functions																	
Manage the Router					rwd	rwd	rwd		d			rwd	rwd	r w d	r w d	rwd	rwd
Set Encryption/Bypass		rwd	rwd					rwd	rw		rwd						
Change Port Adapters																	

The module supports DES (only for legacy systems), DES-MAC, 3DES, 3DES-MAC, SHA-1, MD-5, MD-4, HMAC-SHA-1, HMAC-MD5, Diffie-Hellman, RSA (for digital signatures and encryption (for IKE authentication)), and AES cryptographic algorithms. The MD-5, HMAC-MD5, and MD-4 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-1 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-1 key.
- Internet Key Exchange with RSA-signature authentication.

All pre-shared keys are associated with the Crypto Officer role that created the keys, and the Crypto Officer role is protected by a password. Therefore, the Crypto Officer password is associated with all the pre-shared 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

All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 2 for information on methods to zeroize each key and CSP.

Self-Tests

To prevent secure data from 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 the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Self-tests performed by the IOS image:

- Power-up tests
  - Firmware integrity test
  - RSA signature KAT (both signature and verification)
  - DES KAT
  - TDES KAT
  - AES KAT
  - SHA-1 KAT
  - PRNG KAT
  - Power-up bypass test
  - Diffie-Hellman self-test
  - HMAC-SHA-1 KAT
- Conditional tests
  - Conditional bypass test
  - Pairwise consistency test on RSA signature
  - Continuous random number generator tests

Self-tests performed by the VAM2 (cryptographic accelerator):

- Power-up tests
  - Firmware integrity test
  - RSA signature KAT (both signature and verification)
  - DES KAT
  - TDES KAT
  - AES KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - PRNG KAT
- Conditional tests

- Pairwise consistency test on RSA signature
- Continuous random number generator test

Secure Operation

The Cisco 7206VXR NPE-G1 router with a single VPN Acceleration Module 2 (VAM2) or dual VPN Acceleration Module 2s (VAM2s) meets all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS mode of operation. Operating this router without maintaining the appropriate settings will remove the module from the FIPS approved mode of operation.

Initial Setup

- The Crypto Officer ensures that the VAM2 cryptographic accelerator card is installed in the module by visually confirming the presence of the VAM2 in a port adapter slot.
- The Crypto Officer must apply tamper evidence labels as described in the "Physical Security" section on page 8 of this document.
- Only a Crypto Officer may add and remove port adapters. 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 the "Physical Security" section on page 8 of this document.

System Initialization and Configuration

- The Crypto Officer must perform the initial configuration. The Cisco IOS software version 12.3(3d) is the only allowable image. No other image may be loaded.
- The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the **configure terminal** command line, the Crypto Officer enters the following syntax:

  ```
  config-register 0x0102
  ```

- 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.

- The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
- If the Crypto Officer loads any IOS image onto the router, this will put the router into a non-FIPS mode of operation.
- The I/O controller is not allowed in FIPS mode and should not be installed in the module.

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 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:

- MD-4 and MD-5 for signing
- MD-5 HMAC

Protocols

All SNMP operations must be performed within a secure IPSec tunnel.

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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

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 Ordering tool:

  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 send comments about technical documentation 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, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

Severity 4 (S4)—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- 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://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

This document is to be used in conjunction with the documents that shipped with your hardware.