Cisco Systems, Inc. 7206VXR NPE-G1 and 7301 with VAM2+

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version: Version 1.8

April 3, 2006

INTRODUCTION

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the 7206VXR NPE-G1 and 7301 with VAM2+ from Cisco Systems, Inc., referred to in this document as the modules, routers, or as previously stated. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

This policy was prepared as part of the FIPS 140-2 Level 2 validation of the 7206VXR NPE-G1 and 7301 with VAM2+.

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/.

References

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

- The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- The NIST Cryptographic Module Validation Program website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

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

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

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

7206VXR NPE-G1 AND 7301 WITH VAM2+ FROM CISCO SYSTEMS, INC.

Cisco 7206VXR NPE-G1

Cisco 7206 VXR routers are designed to support gigabit capabilities and to improve data, voice, and video integration in both service provider and enterprise environments. Cisco 7206 VXR routers support a high-speed network processing engine, NPE-G1, and all other available network processing engines.

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

Cisco 7206 VXR routers support the following features:

- Online insertion and removal (OIR)—Add, replace, or remove port adapters without interrupting the system.
- Dual hot-swappable, load-sharing power supplies—Provide 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—Maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.
- Downloadable software—Load new images into Flash memory remotely, without having to physically access the router.

Cisco 7301

The Cisco 7300 Series is optimized for flexible, feature rich IP/MPLS services at the customer network edge, where service providers and enterprises link together. The Cisco 7300 Series can be used for enterprise campus or Internet gateway applications or be deployed by service providers as a high-end CPE router for managed service offerings. Other applications for the Cisco 7301 include: service provider broadband aggregation and metro Ethernet CPE applications.

The compact Cisco 7301 router is the industry's highest performance single rack unit router with million packets per second processing. With 3 built-in Gigabit Ethernet interfaces (copper or optical) and a single slot for any Cisco 7000 Series port adapter the Cisco 7301 is highly flexible for a variety of applications. Additionally for broadband aggregation, the Cisco 7301 supports up to 16,000 subscribers sessions making it ideal for pay-as-you-grow broadband deployment models.

Cisco VPN Acceleration Module 2 PLUS (VAM2+)

The Cisco 7206VXR NPE-G1 and 7301 routers incorporate the VPN Acceleration Module 2+ (VAM2+) cryptographic accelerator card. The 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 and is installed in an available port adapter slot. 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.

Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Validation Level by Section

The Cryptographic Module

The cryptographic boundary for the 7206VXR NPE-G1 with VAM2+ 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 removable port adapter; and the inverse of the three-dimensional space within the case that would be occupied by an installed port adapter. The cryptographic boundary includes the connection apparatus between the port adapter and the motherboard/daughterboard that hosts the port adapter, but the boundary does not include the port adapter itself (except when a VAM2+ is inserted into an available port adapter slot). In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular port adapter (except when a VAM2+ is inserted into an available port adapter interface).

The cryptographic boundary for the 7301 with VAM2+ is the module case. The 7301 has one port adapter slot, which is populated with the VAM2+. The 7206VXR NPE-G1 can support single and dual VAM2+ modules in FIPS mode of operation.

All of the functionality discussed in this document is provided by components within this cryptographic boundary. Each module is a multi-chip standalone module.

Module Interfaces

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables:

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 Port Adapter Interface Power Switch Reset Switch Console Port Auxiliary Port	Control Input Interface
10/100/1000 BASE-TX LAN Port Port Adapter Interface Gigabit Ethernet Port LEDs Console Port Auxiliary Port	Status Output Interface
Power Plug	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces – 7206VXR NPE-G1 with VAM2+

Router Physical Interface	FIPS 140-2 Logical Interface
Gigabit Ethernet 0-2 RJ-45 Ports Gigabit Ethernet 0-2 SFP GBIC Ports Alarm Port Compact Flash Interface Console Port Auxiliary Port	Data Input Interface
Gigabit Ethernet 0-2 RJ-45 Ports Gigabit Ethernet 0-2 SFP GBIC Ports Alarm Port Compact Flash Interface Console Port Auxiliary Port	Data Output Interface

Router Physical Interface	FIPS 140-2 Logical Interface
Gigabit Ethernet 0-2 RJ-45 Ports Gigabit Ethernet 0-2 SFP GBIC Ports Alarm Port Console Port Auxiliary Port	Control Input Interface
Gigabit Ethernet 0-2 RJ-45 Ports Gigabit Ethernet 0-2 SFP GBIC Ports Alarm Port Console Port Auxiliary Port LEDs	Status Output Interface
Power Plug	Power Interface

Table 3 – FIPS 140-2 Logical Interfaces – 7301 with VAM2+

Roles, Services, and Authentication

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 modules can be found in the *Performing Basic System Management* manual and in the online help for the modules.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 characters long, including at least one letter and at least one number. See the Secure Operation section for more information. If 6 integers, one special character and one letter are used without repetition for an 8-digit PIN, the probability of randomly guessing the correct sequence is 1 in 832,000,000. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

User Services

A User enters the system by accessing the console/auxiliary port with a terminal program or via IPSec protected telnet or SSH session to a LAN port. 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**: view state of interfaces and protocols, version of 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

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 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 Port Adapters**: insert and remove adapters in a port adapter slot.

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. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE).

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

CSP NAME	Description	Storage
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)
CSP 2	The public and private exponents used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
CSP 3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
CSP 4	Same as above	DRAM (plaintext)
CSP 5	Same as above	DRAM (plaintext)
CSP 6	Same as above	DRAM (plaintext)
CSP 7	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
CSP 8	The IKE session authentication key. The zeroization is the same as	DRAM

	above.	(plaintext)
CSP 9	The key used to generate IKE skeyid during preshared-key authentication. **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)
CSP 10	This key generates keys 3, 4, 5 and 6. This key is zeroized after generating those keys.	DRAM (plaintext)
CSP 11	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)
CSP 12	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
CSP 13	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
CSP 14	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)
CSP 15	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)
CSP 16	This key is used by the router to authenticate itself to the peer. The key is retrieved from the local database (on the router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
CSP 17	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
CSP 18	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
CSP 19	The ciphertext password of the CO 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)
CSP 20	The RADIUS shared secret. This shared secret is zeroized by executing the “no” form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM (plaintext)
CSP 21	The TACACS+ shared secret. This shared secret is zeroized by executing the “no” form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM (plaintext)
CSP 22	The keys and CSPs above from no. 1 to 21 are located in the router outside from VAM2+. However, the ByteArray key object is located in the RAM of the VAM2+. All key objects of the VAM2+ are built upon the ByteArray key object. The destructor of the ByteArray object uses memset function to overwrite all bytes of the object to 0x00.	DRAM of VAM2+ (plaintext)

Table 4 – Critical Security Parameters

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in Table 5:

SRDI/Role/Service Access Policy	Security Relevant Data Item	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 8	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22
Role/Service																							
User role																							
Status Functions																							
Network Functions		r	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												r w d					r w d						
Define Rules and Filters																							
Status Functions																							
Manage the Router		d													r w d	d		r w d	r w d	r w d	r w d	r w d	r w d
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d		r w							
Change Port Adapters																							

Table 5 – Role and Service Access to CSPs

The module supports Triple-DES, DES-MAC, Triple-DES-MAC, AES, SHA-1, HMAC SHA-1, MD5, HMAC MD5, Diffie-Hellman, cryptographic algorithms. The MD5, HMAC MD5, DES-MAC, and RSA algorithms shall not be used when operating in FIPS mode. Diffie-Hellman can be used; the key agreement, key establishment methodology provides 80 or 96 bits of encryption strength.

> Note: Pursuant to the DES Transition Plan and the approval of the *Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation*, the DES algorithm should not be used in FIPS approved mode of operation.

Each cryptographic implementation has achieved the following certifications:

Algorithm	IOS	VAM2+
AES	Not supported in FIPS mode	173
DES	Not supported in FIPS mode	271*
Triple-DES	Not supported in FIPS mode	275
SHA-1	404	258
SHA-1 HMAC	Not supported in FIPS mode	39
RNG	150	83
RSA	Not supported in FIPS mode	Not supported in FIPS mode

Table 6 - Algorithm Certificates

* This implementation is not used in FIPS mode of operation

The module supports the following key management schemes:

1. Pre-shared key exchange via electronic key entry. DES/Triple-DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
2. Internet Key Exchange method with support for pre-shared keys exchanged and entered electronically.
    - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, Triple-DES or AES keys.
    - The pre-shared key is also used to derive HMAC-SHA-1 key.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO 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. All of the keys and CSPs of the module can be zeroized. Please refer to Table 4 for information on methods to zeroize each key and CSP.

Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly. The modules implement the following power-on self-tests:

Implementation	Tests Performed
IOS	• Software/firmware test • Bypass test • SHA-1 KAT • PRNG KAT • DH Test
VAM2+	• Firmware integrity test • Triple-DES KAT • AES KAT • SHA-1 KAT • HMAC-SHA-1 KAT • PRNG KAT

Table 7 – Module Power On Self Tests

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LANs; this prevents the module from passing any data during a power-on self-test failure.

In addition, the module also provides the following conditional self-tests:

Implementation	Tests Performed
IOS	• Continuous Random Number Generator test for the FIPS-approved RNG • Continuous Random Number Generator test for the non-approved RNGs • Conditional Bypass test
VAM2+	• Continuous Random Number Generator test for the FIPS-approved RNG • Continuous Random Number Generator test for the non-approved RNGs

Table 8 - Module Conditional Self Tests

SECURE OPERATION OF THE 7206VXR NPE-G1 AND 7301 WITH VAM2+

These routers meet all the applicable 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. All configuration activities must be performed via the command line interface via the console (for initial configuration) or IPSec protected SSH or telnet sessions – neither the web configuration tools CSRW or SDM may be used.

System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. The following IOS versions are the only allowable image; no other image may be loaded

   7206VXR NPE-G1 with VAM2+: c7200-jk9o3s-mz.123-11.T10 (IOS version 12.3(11)T10)
   7301 with VAM2+: c7301-jk9o3s-mz.123-11.T10 (IOS version 12.3(11)T10)

2. 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
   ```

3. The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 characters, including at least one letter and at least one number, 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]
   ```

4. The Crypto Officer must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary 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
   ```

5. The Crypto Officer should not assign users to privilege level other than Level 1 (the default).
6. 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, including at least one letter and at least one number.
7. The Crypto Officer must apply tamper evidence labels as described later in this document.
8. The module must be configured to only use hardware acceleration. As such if there is a failure in the VAM2+ card, the module is considered to be out of FIPS-Approved Mode of operation. A failure in the integrity check for VAM2+ will be indicated via the following console message:

   ```
   <DATE>: %VPN_HW-1-INITFAIL: Slot <SLOT NUMBER>: File doesn't verify
   ```

```
<DATE>: %VPN_HW-1-INITFAIL: Slot <SLOT NUMBER>: microcode download
failure
```

The status of the VAM2+ can also be verified with the "`show crypto engine config`"command.

Note: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

Note: For an overview of the VAM2+ LEDs, please refer to the Installation and Configuration Guide at:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_and_configuration_guide_chapter09186a0080369590.html#wp1033479

IPSec Requirements and Cryptographic Algorithms

1. The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).
2. 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-sha-hmac
    - esp-3des
    - esp-aes
3. The following algorithms should not be used:
    - MD-5 for signing
    - MD-5 HMAC
    - DES
    - Software implementations of AES, Triple-DES, SHA-1 HMAC, and RSA

Protocols

1. 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.
2. Secure DNS is not allowed in FIPS mode of operation and should not be configured.

Remote Access

1. 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, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

2. SSH access to the module is not allowed in FIPS approved mode of operation.

Tamper Evidence

Any port adapter slot not populated with a port adapter must be populated with an appropriate slot cover in order to operate in a FIPS compliant mode. The slot covers are included with each router, and additional covers may be ordered from Cisco. The same procedure mentioned below to apply tamper evidence labels for port adapters must also be followed to apply tamper evidence labels for the slot covers.

7206VXR NPE-G1 with VAM2+

The front of the router provides 6 port adapter slots, and the rear of the router provides on-board LAN connectors, PC Card slots, and Console/Auxiliary connectors. The power cable connection, a power switch, and the access to the Network Processing Engine are at the rear of the router.

Any port adapter slot that is not populated with a port adapter must be populated with an appropriate slot cover in order to operate in a FIPS compliant mode. The slot covers are included with each router, and additional covers may be ordered from Cisco. The same procedure mentioned below to apply tamper evidence labels for port adapters must also be followed to apply tamper evidence labels for the slot covers. Once the router has been configured to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. The Crypto Officer should be instructed to record serial numbers, and to inspect for these signs of tampering or changed numbers periodically.

To seal the system, apply serialized tamper-evidence labels as depicted in Figure 1 and
Figure 2 below and as follows:

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 10°C, otherwise the labels may not properly cure.
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.
3. A tamper evidence label should be placed over the Compact Flash card slot on the NPE-G1.
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.
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.
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.
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.
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.

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.
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.
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.
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.
13. Allow the labels to cure for five minutes.

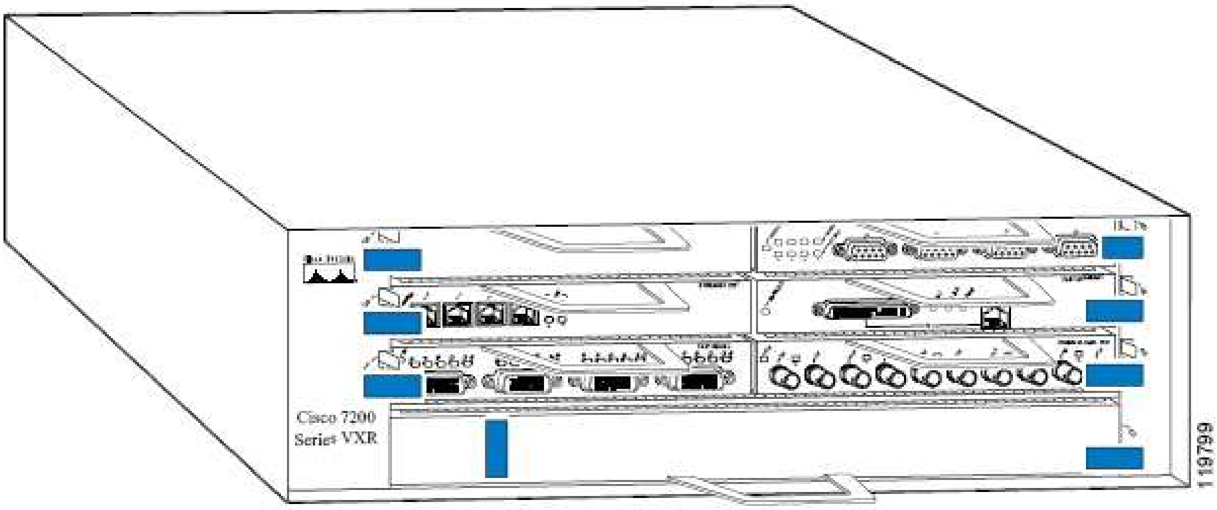

Figure 1 - 7206VXR (Front) Tamper Evident Label Placement

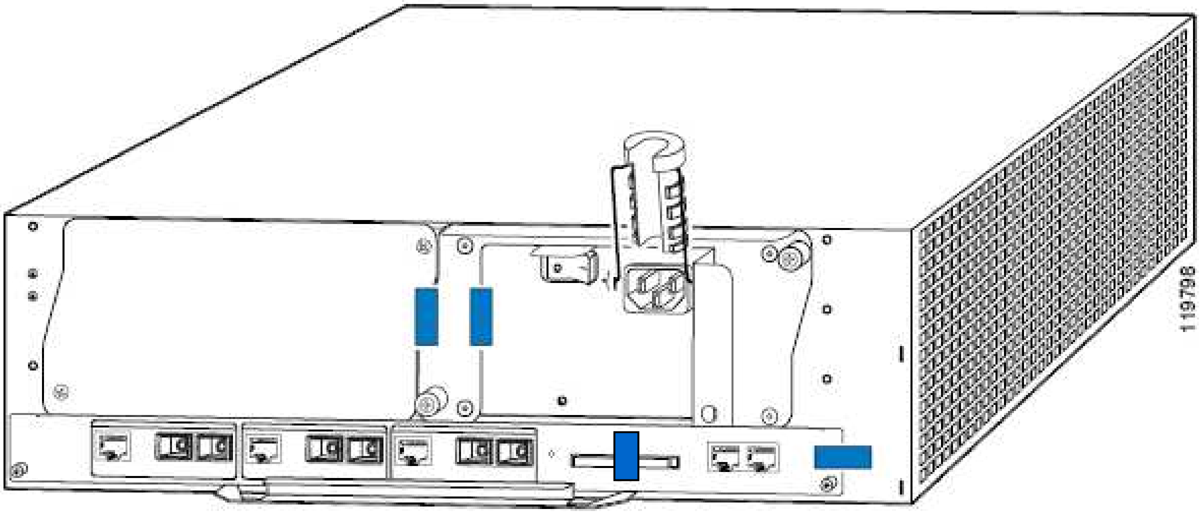

Figure 2 - 7206VXR (Back) Tamper Evident Label Placement

7301 with VAM2+

To seal the system, apply serialized tamper-evidence labels as depicted in Figure 3 below and as follows:

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 10°C, otherwise the labels may not properly cure.
2. A tamper evidence label should be placed over the Compact Flash card slot.
3. A tamper evidence label should be placed so that one half of the label covers the top of the enclosure and the other half covers the port adapter slot.
4. A tamper evidence label should be placed so that one half of the label covers the top of the enclosure and the other half covers the side.
5. Allow the labels to cure for five minutes.

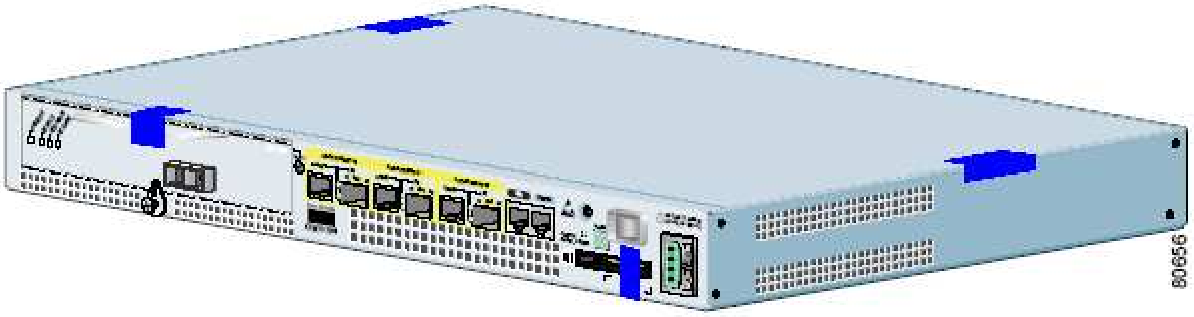

Figure 3 - 7301 (Front) Tamper Evident Label Placement

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the module cover. Since the tamper evident 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 with. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices.

Definition List

AES	Advanced Encryption Standard
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test

LED	Light Emitting Diode
NPE	Network Processing Engine
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
VAM	VPN Acceleration Module